Department of Homeland Security

Information Analysis and Infrastructure Protection Directorate

CyberNotes

Issue #2003-13 *June 30, 2003*

CyberNotes is published every two weeks by the Department of Homeland Security/Information Analysis and Infrastructure Protection (IAIP) Directorate. Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between June 11 and June 29, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
123Apps[1]	Windows	ASP Chat	A vulnerability exists in the 'login' variable due to insufficient validation of user-supplied nickname values, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	ASP Chat Login Nickname	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Abuse-SDL[2]	Multiple	Abuse-SDL 0.7.0	A buffer overflow vulnerability exists due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Abuse-SDL Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[1] Exploitlabs.com Advisory, EXPL-A-2003-008, June 16, 2003.
[2] SecurityFocus, June 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
ACLogic[3]	Multiple	CesarFTP	A remote Denial of Service vulnerability exists in the 'CWD' command when a malicious user submits excessive data as the argument.	No workaround or patch available at time of publishing.	CesarFTP Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Aladdin Enterprises[4, 5, 6] ***RedHat issues another advisory[7]***	**Unix**	**Ghostscript 5.10.10, 5.10.15, 5.10.16, 5.50, 5.50.8, 6.51-6.53, 7.0 4-7.0 6**	**A vulnerability exists when Ghostscript is used to process specially formatted PS files, which could let a malicious user execute arbitrary commands.**	**Upgrade available at: http://prdownloads.sourceforge.net/ghostscript/ghostscript-7.07.tar.gz?download** **Mandrake: http://www.mandrakesecure.net/en/ftp.php** **OpenPKG: ftp.openpkg.org** **RedHat: ftp://updates.redhat.com/** **Sun: ftp://ftp.cobalt.sun.com/pub/products/sunlinux/5.0/en/updates/i3**	**GhostScript Arbitrary Command Execution** **CVE Name: CAN-2003-0354**	**High**	**Bug discussed in newsgroups and websites.**
Alberto Pittoni[8]	Windows, Unix	Alguest 1.1b, 1.1c	A vulnerability exists because authentication can be bypassed with a fake cookie, which could let an unauthorized malicious user obtain administrative access.	No workaround or patch available at time of publishing.	Alguest Authentication Bypass	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Alt-N[9]	Windows	WebAdmin 2.0 0- 2.0.4	A buffer overflow vulnerability exists in the 'USER' parameter due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.altn.com/WebAdmin/Release/wa205_en.exe	WebAdmin USER Parameter Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Apple[10]	MacOS X	MacOS X Server 10.2.6	A vulnerability exists in the 'dsimportexport' utility, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.info.apple.com/kbnum/n120215	Mac OS X Information Disclosure CVE Name: CAN-2003-0420	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[3] SecurityFocus, June 18, 2003.
[4] Red Hat Security Advisory, RHSA-2003:181-01, May 30, 2003,
[5] OpenPKG Security Advisory, OpenPKG-SA-2003.030, June 3, 2003.
[6] Mandrake Linux Security Update Advisory, MDKSA-2003:065, June 10, 2003.
[7] Red Hat Security Advisory, RHSA-2003:182-04, June 17, 2003.
[8] SecurityFocus, June 18, 2003.
[9] NGSSoftware Insight Security Research Advisory, NISR2406-03, June 24, 2003.
[10] Apple Security Update, 61798, June 16, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Avaya[11]	Multiple	Cajun P130 Series Firmware 2.9.1, P133 Series Firmware 2.6.1, P330 Series Firmware 3.8.1, 3.8.2, 3.9.1, 3.10, 3.11, 3.12.1, P333 Series Firmware 3.12.0, G700 Media Gateway 3.x	A remote Denial of Service vulnerability exists because traffic to port 4000 is not properly handled.	Avaya has addressed this issue for the P330 in version 4.0 of the firmware. Further information can be obtained by contacting the vendor.	Cajun Network Switch Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required however a Proof of Concept exploit has been published.
Bill Wilson[12]	Unix	GKrellM 2.1.13	A buffer overflow vulnerability exists due to insufficient bounds checking of network based data, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Gkrellmd Remote Buffer Overflow	High	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Central Command[13] ***Upgrade now available*** [14]	**Unix**	**Vexira Antivirus for Linux 2.1.7**	**A buffer overflow vulnerability exists when an overly long commandline argument is submitted to the Vexira binary, which could let a malicious user execute arbitrary code.**	***The vendor has addressed this issue in version 2.1.7.21 of Vexira Antivirus. Users are advised to upgrade by issuing the following command:*** ***vexira --update***	**Vexira Antivirus Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**
Compaq Computer Corporation[15]	Windows	Web-Based Management Agent	Several vulnerabilities exist: a remote Denial of Service vulnerability exists when a malicious user submits malformed requests; a remote Denial of Service vulnerability exists when handling malformed GET requests; and a remote file verification vulnerability exists which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Web-Based Management Agent Multiple Remote Vulnerabilities	Low/ Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser. Proof of Concept exploit has been published.

[11] Bugtraq, June 18, 2003.
[12] SecurityFocus, June 24, 2003.
[13] Securiteam, April 18, 2003.
[14] SecurityFocus, June 17, 2003.
[15] SecurityFocus, June 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Crob Software Studio [16] ***Upgrade now available*** [17]	**Windows**	**Crob FTP Server 2.50.4**	**A vulnerability exists in the 'USER' command due to invalid format specifiers, which could let a remote malicious user execute arbitrary code.**	***Upgrade available at:*** **http://www.crob.net/studio/ftpserver/**	**Crob FTP Server Remote Username Format String**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.**
Dantz Development Corp. [18]	Unix	Client 5.0.540	A vulnerability exists because some files and directories are created with insecure permissions, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	Client Insecure Default Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Deerfield [19]	Windows	VisNetic WebMail 5.8.6 .6	An information disclosure vulnerability exists when the dot character is appended to the end of an URI request, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	VisNetic WebMail Information Disclosure	Medium	Bug discussed in newsgroups and websites. Exploits have been published.
Dr. Jay Stockman [20] ***Exploit script has been published.*** [21]	**Multiple**	**Stockman Shopping Cart 7.8**	**A vulnerability exists in the 'shop/plx' script due to insufficient sanitization of user-supplied URI parameters, which could let a remote malicious user execute arbitrary code.**	**No workaround or patch available at time of publishing.**	**Stockman Shopping Cart Arbitrary Command Execution**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**
Dune[22]	Unix	Dune 0.6.7	A buffer overflow vulnerability exists when an overly long GET request is submitted, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Dune Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Eldav[23]	Unix	Eldav 0.7.0	A vulnerability exists because temporary files are created without appropriate security precautions, which could let a malicious user obtain elevated privileges.	Upgrade available at: http://www.gohome.org/eldav/eldav-0.7.2.tar.gz **Debian:** http://security.debian.org/pool/updates/main/e/eldav/	ELDAV Insecure Temporary File CVE Name: CAN-2003-0438	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[16] Securiteam, June 2, 2003.
[17] SecurityFocus, June 23, 2003.
[18] Bugtraq, June 16, 2003.
[19] Tripbit Security Advisory, TA-2003-06, June 23, 2003.
[20] SecurityFocus, May 1, 2003.
[21] SecurityFocus, June 17, 2003.
[22] ISS Security Alert Summary, AS03-25, June 24, 2003.
[23] Debian Security Advisory, DSA 325-1, June 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Elm Development Group[24]	Unix	ELM 2.3, 2.4	A buffer overflow vulnerability exists in the 'TERM' environment variable due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Elm Local TERM Environment Variable Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Enstar [25]	Windows	Mailtraq 2.1 .0.1302	Several vulnerabilities exist: a Directory Traversal vulnerability exists which could let a remote malicious user obtain sensitive information; a vulnerability exists because passwords are stored using a weak encoding algorithm, which could let a malicious user obtain sensitive information; a remote Denial of Service vulnerability exists when a malicious user submits a specially crafted string with MAIL FROM, RCPT TO, HELO, or FROM SMTP commands; a remote Denial of Service vulnerability exists in the authentication CGI script when a malicious user submits a long username and/or password; and a vulnerability exists when displaying the 'Subject' file of an e-mail message due to insufficient filtering of HTML code, which could let a remote malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Mailtraq Remote Directory Traversal	Low/ Medium/ **High** **(Low if a DoS; Medium if sensitive information can be obtained; and High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required for the Cross-Site Scripting or HTML filtering vulnerabilities. Exploit script has been published for the weak encoding vulnerability.
Ethereal Group[26] ***Vendors release advisories*** [27, 28]	**Windows 95/98/ME/ NT 4.0/2000, XP, Unix**	**Ethereal 0.8, 0.8.18, 0.9.0-0.9.11**	**Buffer overflow vulnerabilities exist in several dissectors that are included with Ethereal due to integer overflows and off-by-one errors, which could let a remote malicious user execute arbitrary code.**	**Upgrade available at:** **http://www.ethereal.com/distribution/ethereal-0.9.12.tar.gz** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***Debian:*** **http://security.debian.org/pool/updates/main/e/ethereal/**	**Ethereal Multiple Dissector Buffer Overflows**	**High**	**Bug discussed in newsgroups and websites.**

[24] SecurityFocus, June 24, 2003.
[25] Securiteam, June 16, 2003.
[26] Ethereal Security Advisory, enpa-sa-00009, May 3, 2003.
[27] Debian Security Advisory, DSA 313-1, June 12, 2003.
[28] Mandrake Linux Security Update Advisory, MDKSA-2003:067, June 16, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Ethereal Group[29] *Vendors issue advisories*[30, 31, 32]	Windows 95/98/ME/ NT 4.0/2000, XP, Unix	Ethereal 0.9.0-0.9.12	Multiple vulnerabilities exist: a vulnerability exists in the DCERPC dissector when decoding certain NDR strings, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a vulnerability exists in the SPNEGO dissector when parsing certain ASN.1 codes, which could let a remote malicious user cause a Denial of Service; a buffer overflow vulnerability exists in the OSI dissector when handling bad IPv4 or IPv6 prefix lengths due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the BGP, WTP, DNS, 802.11, ISAKMP, WSP, CLNP, ISIS, and RMI dissectors because certain strings are not properly handled, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; and a vulnerability exists in the tvb_get_nstringz0() routine because a zero-length buffer size is incorrectly handled, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	Upgrade available at: http://www.ethereal.com/distribution/ethereal-0.9.13.tar.gz *Debian:* http://security.debian.org/pool/updates/main/e/ethereal/ *Mandrake:* http://www.mandrakesecure.net/en/ftp.php *Conectiva:* ftp://atualizacoes.conectiva.com.br/	Ethereal Multiple Vulnerabilities CVE Names: CAN-2003-0428, CAN-2003-0429, CAN-2003-0431, CAN-2003-0432	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.

[29] Ethereal Advisory, enpa-sa-00010, June 11, 2003.
[30] Debian Security Advisory, DSA 324-1, June 18, 2003.
[31] Mandrake Linux Security Update Advisory, MDKSA-2003:070, June 23, 2003.
[32] Conectiva Linux Security Announcement, CLA-2003:662, June 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Ethereal Group[33] ***Debian issues upgrades***[34]	**Windows 95/98/ME/ NT 4.0/2000, XP, Unix**	**Ethereal 0.9.0-0.9.12**	**Multiple vulnerabilities exist: a vulnerability exists in the DCERPC dissector when decoding certain NDR strings, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a vulnerability exists in the SPNEGO dissector when parsing certain ASN.1 codes, which could let a remote malicious user cause a Denial of Service; a buffer overflow vulnerability exists in the OSI dissector when handling bad IPv4 or IPv6 prefix lengths due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the BGP, WTP, DNS, 802.11, ISAKMP, WSP, CLNP, ISIS, and RMI dissectors because certain strings are not properly handled, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; and a vulnerability exists in the tvb_get_nstringz0() routine because a zero-length buffer size is incorrectly handled, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.**	**Upgrade available at:** **http://www.ethereal.com/distribution/ethereal-0.9.13.tar.gz** ***Debian:*** **http://security.debian.org/pool/updates/main/e/ethereal/e**	**Ethereal Multiple Vulnerabilities** **CVE Names: CAN-2003-0428, CAN-2003-0429, CAN-2003-0430, CAN-2003-0431, CAN-2003-0432**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites.**
FakeBO[35]	Windows, Unix	FakeBO 0.4.1	A format string vulnerability exists in the syslogprintf() function, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	FakeBO syslogprintf() Format String	High	Bug discussed in newsgroups and websites.
Frassetto Software[36]	Windows	Armida Databased Web Server 1.0	A remote Denial of Service vulnerability exists when processing malicious GET requests. It may also be possibly to execute arbitrary code.	No workaround or patch available at time of publishing.	Armida Databased Web Server Remote Denial of Service	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[33] Ethereal Advisory, enpa-sa-00010, June 11, 2003.
[34] Debian Security Advisory DSA 324-1, June 18, 2003.
[35] SecurityTracker Alert ID, 1006973, June 12, 2003.
[36] Tripbit Security Advisory, TA-2003-06, June 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
FreeWnn[37]	Unix	FreeWnn 1.1.1	A vulnerability exists in the logging option, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	FreeWnn JServer Logging Option Data Corruption	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Fungus Eye Entertainment[38]	Windows	Methodus 3 Build 9	A file disclosure vulnerability exists due to insufficient checking of HTTP GET requests, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Methodus 3 FTP Server File Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via an FTP client.
Gnocatan[39]	Unix	Gnocatan 0.6.1	Several buffer overflow vulnerabilities exist due to boundary errors, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/g/gnocatan/	Multiple Gnocatan Server Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
GNU[40]	Unix	GNATS 3.113, 3.113.1	A buffer overflow vulnerability exists when certain environment variables are parsed, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	GNATS Environment Variable Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
GNU[41] ***Vendors issue advisories*** [42, 43, 44, 45, 46] ***RedHat issues another advisory***[47]	**Unix**	**GNU Privacy Guard 1.0-1.2.1**	**A vulnerability exists in the key validation code due to insufficient differentiation between the validity given to individual IDs on a public key that has multiple user IDs linked to it, which could let a malicious user obtain sensitive information.**	**Upgrade available at:** **http://www.gnupg.org/(en)/download/index.html#auto-ref-0** ***Engarde:*** **http://infocenter.guardiandigital.com/advisories/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***OpenPKG:*** **ftp.openpkg.org** ***RedHat:*** **ftp://updates.redhat.com/** ***Sun:*** **http://sunsolve.sun.com/patches/linux/security.html** ***YellowDog:*** **ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/**	**GNU Privacy Guard Insecure Trust Path To User ID** **CVE Name: CAN-2003-0255**	**Medium**	**Bug discussed in newsgroups and websites.**

[37] SecurityFocus, June 14, 2003.
[38] SecurityTracker Alert ID, 1006980, June 13, 2003.
[39] Debian Security Advisory, DSA 315-1, June 11, 2003.
[40] INetCop Security Advisory, 2003-0x82-018, June 21, 2003.
[41] Bugtraq, May 4, 2003.
[42] Guardian Digital Security Advisory, ESA-20030515-016, May 15, 2003.
[43] OpenPKG Security Advisory, OpenPKG-SA-2003.029, May 16, 2003.
[44] Red Hat Security Advisory, RHSA-2003:175-01, May 21, 2003.
[45] Mandrake Linux Security Update Advisory, MDKSA-2003:061, May 22, 2003.
[46] Yellow Dog Linux Security Announcement, DU-20030602-4, June 2, 2003.
[47] Red Hat Security Advisory, RHSA-2003:176-06, June 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
GNU[48]	Unix	GNATS 3.0 02	Multiple buffer overflow vulnerabilities exist: a vulnerability exists in the 'pr-edit' utility due to insufficient bounds checking on the arguments to the '-d' commandline option, which could let a malicious user execute arbitrary code; and a vulnerability exists in the 'pr-edit' utility when a file is locked for reading due to improper use of fscanf(), which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	GNATS Buffer Overflows	High	Bug discussed in newsgroups and websites. Bug discussed in newsgroups and websites. Proof of Concept exploit script has been has been published.
Happycgi.com[49] ***Exploit script has been published.***[50]	**Unix**	**HappyMall 4.3, 4.4**	**A vulnerability exists in the ‘‘normal_html.cgi’ and 'member_html.cgi' scripts due to insufficient filtering of user-supplied input, which could let a remote malicious user execute arbitrary commands.**	**Patch available at:** **http://happymall.happycgi.com/forum/forum_detail.cgi?thread=353**	**HappyMall E-Commerce Software Remote Arbitrary Command Execution** **CVE Name: CAN-2003-0243**	**High**	**Bug discussed in newsgroups and websites. Exploits have been published.** ***Exploit script has been published.***
Hewlett Packard Company[51] ***Workaround available***[52]	**Unix**	**HP-UX 10.20**	**A buffer overflow vulnerability exists in the 'pcltotiff' program due to insufficient bounds checking, which could let a malicious user execute arbitrary code.**	***Workaround:* *Remove set group id permissions from pcltotiff and allow read access to /usr/lib/X11/fonts/ifo.st/typefaces/ by executing the following commands as the root user:*** ***/sbin/chmod 555 /opt/sharedprint/bin/pcltotiff*** ***/sbin/chmod o+r /usr/lib/X11/fonts/ifo.st/typefaces/***	**HPUX PCLToTIFF Command Line Argument Local Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites.**
Hewlett Packard Company[53]	Unix	HP-UX 11.0, 11.11, 11.22	A remote Denial of Service vulnerability exists in the TFTPD implementation when certain network traffic is processed.	Patches available at: ftp://tftpd:tftpd@hprc.external.hp.com/	HP-UX TFTPD Remote Denial of Service	Low	Bug discussed in newsgroups and websites.

[48] INetCop Security Advisory, 2003-0x82-018, June 21, 2003..
[49] Korean CERT Advisory, KA-2003-33, May 3, 2003.
[50] SecurityFocus, June 17, 2003.
[51] Bugtraq, June 9, 2003.
[52] Bugtraq, June 20, 2003.
[53] Hewlett-Packard Company Security Bulletin, HPSBUX0306-266, June 18, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
HTML Helper[54]	Windows	Power Server 1.0	Several vulnerabilities exist: a remote Denial of Service vulnerability exists when malformed 'USER' and 'PASS' commands are processed; a vulnerability exists because usernames and passwords are stored in plaintext, which could let a remote malicious user obtain sensitive information; a remote Denial of Service vulnerability exists when a malicious user submits malformed GET requests; a Directory Traversal vulnerability exists because FTP Addon does not properly handle some types of requests, which could let a remote malicious user obtain sensitive information; and a vulnerability exists because arbitrary passwords are accepted when a valid username is supplied, which could let a remote malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	Power Server Multiple Vulnerabilities	Low/ Medium (Medium if unauthorized access or sensitive information can be obtained)	Bug discussed in newsgroups and websites. There is no exploit code required.
IBM[55]	Unix	HACMP 4.4, 4.4.1	A Denial of Service vulnerability exists due to the 'clstrmgr' service failing to correctly handle TCP RST packets.	Upgrade available at: http://www-1.ibm.com/support/docview.wss?uid=isg1IY23867	IBM HAES/ HACMP RST Packet Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability can be exploited using publicly available port scanning tools.
IBM[56]	OS/390, z/OS	OS/390 V2R9, V2R6, RACF 1.1-1.7, 1.9, 2.1, 2.2, RACF/MVS 1.7, 1.8, 1.8.1, 1.9.2, IBM z/OS	A vulnerability exists in the Resource Access Control Facility (RACF) when mapping profiles are updated, which could let a malicious user obtain elevated privileges.	**Workaround:** IBM has said that this issue can be resolved by correcting the UNIXMAP profiles. This can be done by calling the PERMIT command. **Solution:** IBM has released APAR OA02696 to address this issue. Users/administrators can obtain further information by contacting the vendor.	IBM RACF Profile Updating Privilege Elevation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[54] Securiteam, June 19, 2003.
[55] SecurityFocus, June 13, 2003.
[56] IBM Advisory, MSS-OAR-E01-2003.0, June 17, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Indigo STAR Software[57]	Windows, Unix	PerlEdit 1.07	A remote Denial of Service vulnerability exists when a connection is made to TCP port 1956.	No workaround or patch available at time of publishing.	PerlEdit Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Infobot[58]	Unix	Infobot 0.45.3	A vulnerability exists because the default installation enables two default user accounts, which could let a remote malicious user obtain unauthorized access..	No workaround or patch available at time of publishing.	Infobot Default Installation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Internet Security Systems[59]	Multiple	BlackICE Defender 3.6 cbd	A vulnerability exists in the detection of cross-site scripting vulnerabilities when embedded within various HTTP requests, which could let a malicious user evade intrusion detection while carrying out these attacks against a target system.	No workaround or patch available at time of publishing.	BlackICE Defender Cross-Site Scripting Detection Evasion	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Ivan et al Stepnikov [60]	Unix	MidHost-ing FTPd 1.0.1	A Denial of Service vulnerability exists because shared memory is not properly implemented when the 'm' flag (-m) is enabled.	No workaround or patch available at time of publishing.	MidHosting FTP Daemon Shared Memory Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Jani Ollikai-nenv[61]	Unix	Typespeed 0.4, 0.4.1	A vulnerability exists in the 'net_swapscore()' function due to insufficient bounds checking, which could let a malicious user execute arbitrary code with elevated privileges.	**Debian:** http://security.debian.org/pool/updates/main/t/typespeed/	Typespeed Arbitrary Code Execution CVE Name: CAN-2003-0435	**High**	Bug discussed in newsgroups and websites.
Jnethack / Nethack[62, 63]	Unix	Jnethack 1.1.5, 1.1.3; Nethack 3.3.0, 3.4.0	Several vulnerabilities exist: a buffer overflow vulnerability exists in the '-s' command line option, which could let a malicious user obtain elevated privileges; and a vulnerability exists due to weak default permissions, which could let a malicious user execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/j/jnethack/	Nethack / Jnethack Incorrect Permissions CVE Names: CAN-2003-03589, CAN-2003-0359	Medium	Bug discussed in newsgroups and websites.

[57] Exploitlabs.com Advisory, EXPL-A-2003-010, June 21, 2003.
[58] Exploitlabs.com Advisory, EXPL-A-2003-007, June 14, 2003.
[59] SecurityFocus, June 17, 2003.
[60] Bugtraq, June 18, 2003.
[61] Debian Security Advisory, DSA 322-1, June 16, 2003.
[62] Debian Security Advisory, DSA 316-1, June 11, 2003.
[63] Debian Security Advisory, DSA 316-3, June 17, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
KDE[64] ***Upgrades now available*** [65, 66] ***RedHat issues another advisory***[67]	**Unix**	**Konqueror Embedded 0.1**	**A vulnerability exists because the Common Name (CN) field on X.509 certificates is not properly validated when a SSL/TLS session is negotiated, which could let a malicious server masquerade as a trusted server.**	***KDE:*** **ftp://ftp.kde.org/pub/kde/security_patches** ***RedHat:*** **ftp://updates.redhat.com/**	**Konqueror Embedded Common Name Certificate Validation** **CVE Name: CAN-2003-0370**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
Kerio Technol-ogies[68]	Windows NT 4.0/2000, XP	Mailserver 5.6.3	Multiple vulnerabilities exist: several Cross-Site Scripting vulnerabilities exist in the 'add_acl,' and 'do_map,' modules, which could let a remote malicious user execute arbitrary code; and several buffer overflow vulnerabilities exists when handling usernames of excessive length due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	MailServer Cross-Site Scripting & Buffer Overflows	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published for the Cross-Site Scripting vulnerabilities. An exploit script for the buffer overflow vulnerabilities has been published.
Ledscripts .com[69]	Windows, Unix	LedNews 0.7	A Cross-Site Scripting vulnerability exists in news posts due to insufficient filtering, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	LedNews Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Linux-PAM Project[70]	Unix	Linux-PAM 0.77	A vulnerability exists in the 'pam_wheel' module due to the way users are authenticated, which could let a malicious user obtain root access.	Upgrade available at: http://cvs.sourceforge.net/cgi-bin/viewcvs.cgi/pam/Linux-PAM/	Linux-PAM Pam_Wheel Module CVE Name: CAN-2003-0388	**High**	Bug discussed in newsgroups and websites. There is no exploit code required. Proof of Concept exploit has been published.

[64] Bugtraq, May 7, 2003.
[65] KDE Security Advisory, June 2, 2003.
[66] Red Hat Security Advisory, RHSA-2003:192-01, June 5, 2003.
[67] Red Hat Security Advisory, RHSA-2003:193-08, June 17, 2003.
[68] Securiteam, June 19, 2003.
[69] SecurityTracker Alert ID, 1006995, June 16, 2003.
[70] iDEFENSE Security Advisory, June 16, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Lyskom[71]	Unix	Lyskom 2.0.0-2.0.7	A Denial of Service vulnerability exists when an unauthenticated malicious user submits a large query.	**Debian:** http://security.debian.org/pool/updates/main/l/lyskom-server/	Lyskom Server Unauthenticated User Denial of Service CVE Name: CAN-2003-0366	Low	Bug discussed in newsgroups and websites.
Michael Speck[72]	Unix	lbreakout2 2.0-2.5	A format string vulnerability exists, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	LBreakOut2 Remote Format String	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft [73]	Windows 2000	Windows 2000 Advanced Server, SP1-SP4, 2000 Datacenter Server, SP1- SP4, 2000 Server, SP1- SP4	A buffer overflow vulnerability exists in the way 'nsiislog.dll' processes incoming client requests, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-022.asp	Windows Media Services NSIISlog.DLL Remote Buffer Overflow CVE Name: CAN-2003-0349	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft [74]	Windows 95/98/ME/ NT 4.0/2000, 2003	Internet Explorer 5.5, SP1&SP2, 6.0	A vulnerability exists due to an input validation error in the handling of XML files, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Internet Explorer MSXML XML File Parsing	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft [75]	Windows 95/98/ME/ NT 4.0/2000, 2003	Internet Explorer 5.0.1, SP1-SP3, 5.5, SP1&SP2, 6.0, SP1	A vulnerability exists when custom HTTP error messages are displayed due to an input validation error, which could let a remote malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Internet Explorer Custom HTTP Error Messages	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft [76]	Windows 95/98/ME/ NT 4.0/2000, 2003	Internet Explorer 5.0, 5.0.1, SP1-SP3, 5.5, SP1& SP2, 6.0, SP1	A buffer overflow vulnerability exists when the 'Align' attribute of the 'HR' tag is given an excessive value, which could let a remote malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	Internet Explorer Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[71] Debian Security Advisory, DSA 318-1, June 13, 2003.
[72] Bugtraq, June 24, 2003.
[73] Microsoft Security Bulletin, MS03-022, June 25, 2003.
[74] GreyMagic Security Advisory GM#013-IE, June 17, 2003.
[75] GreyMagic Security Advisory GM#014-IE, June 17, 2003.
[76] Bugtraq, June 22, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [77]	Windows 95/98/ME/ NT 4.0/2000, XP, 2003	Windows Media Player 9.0	A vulnerability exists due to insufficient validation of requests made to the ActiveX control, which could let a malicious user obtain sensitive information.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-021.asp	Media Player 9 Unauthorized Media Library Access CVE Name: CAN-2003-0348	Medium	Bug discussed in newsgroups and websites.
Mike Bryeans[78]	Windows NT 4.0	WebBBS Pro 1.18	A remote Denial of Service vulnerability exists when a malformed HTTP request is submitted.	No workaround or patch available at time of publishing.	WebBBS Pro Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
mikmod[79]	Unix	mikmod 3.1.6	A buffer overflow vulnerability exists due to improper handling of long file names when opening archives, which could let a remote malicious user obtain unauthorized privileges.	**Debian:** http://security.debian.org/pool/updates/main/m/mikmod/	MikMod Long File Name Local Buffer Overflow CVE Name: CAN-2003-0427	Medium	Bug discussed in newsgroups and websites.
Mini HTTP Server[80]	Multiple	WebForum Server 1.0	A Directory Traversal vulnerability exists because some types of files are not handled properly, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	WebForums Remote Directory Traversal	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Miquel van Smoorenburg[81, 82]	Unix	Cistron Radius 1.6.4-1.6.6	A buffer overflow vulnerability exists when a long specially crafted NAS-Port attribute is submitted, which could let a remote malicious user execute arbitrary code.	**SuSE:** ftp://ftp.suse.com/pub/suse/ **Debian:** http://security.debian.org/pool/updates/main/r/radiusd-cistron/	Cistron RADIUS Buffer Overflow NAS-Port Attribute	**High**	Bug discussed in newsgroups and websites.
Mollensoft Software[83]	Windows	Enceladus Server Suite 3.9.11, Hyperion FTP Server 3.5.2	Multiple vulnerabilities exist due to insufficient bounds checking of user-supplied command parameters, which could let a malicious user cause a Denial of Service and potentially execute arbitrary code with SYSTEM privileges.	No workaround or patch available at time of publishing.	Hyperion FTP/Enceladus Server Suite Multiple Remote Heap Corruption	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[77] Microsoft Security Bulletin, MS03-021, June 25, 2003.
[78] Secunia Security Advisory, June 13, 2003.
[79] Debian Security Advisory, DSA 320-1, June 13, 2003.
[80] SecurityFocus, June 18, 2003.
[81] SuSE Security Announcement, SuSE-SA:2003:030, June 13, 2003.
[82] Debian Security Advisory, DSA 321-1, June 13, 2003.
[83] SecurityFocus, June 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mollen-soft Software[84]	Windows	Enceladus Server Suite 2.6.1, 3.9, 3.9.11	Multiple vulnerabilities exist: a Cross-Site Scripting vulnerability exists due to insufficient sanitization of HTML code, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists in the '\ProgramFiles\enceladus\users' folder because usernames and passwords are stored in plaintext, which could let a malicious user obtain sensitive information; and a vulnerability exists because a remote malicious user can download the .htaccess file that contains usernames and hashed passwords.	No workaround or patch available at time of publishing.	Enceladus Server Suite Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.
MRV Commun-ications, Inc.[85]	Multiple	OptiSwitch 800, 400	A vulnerability exists when a specific sequence of key presses is initiated, which could let a remote malicious user obtain root access.	No workaround or patch available at time of publishing.	OptiSwitch 400/800 Unauthorized Remote Root Access	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Multiple Vendors[86]	Multiple	Exploit Labs Wood's Infinity Scan EZ 3.69; The Infinity Project Infinity CGI Exploit Scanner 3.11 Beta	Several vulnerabilities exist: a Cross-Site Scripting vulnerability exists, which could let a malicious user execute arbitrary HTML and script code; a vulnerability exists due to an input validation error in the pattern matching of hostnames, which could let a malicious user bypass security policies; and a vulnerability exists due to insufficient sanitization of input supplied via URI parameters, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Infinity CGI Exploit Scanner Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit has been published for the Cross-Site Scripting vulnerability. There is no exploit code required for the security policy bypass vulnerability.
Multiple Vendors[87]	Unix	Linux kernel 2.2-2.2.25, 2.4.1-2.4.21	An information disclosure vulnerability exists in the /proc filesysttem when setuid applications are invoked, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Linux /proc Filesystem Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[84] Securiteam, June 16, 2003.
[85] Bugtraq, June 25, 2003.
[86] SecurityFocus, June 13, 2003.
[87] Bugtraq, June 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [88, 89] *More advisories issued*[90, 91]	**Unix**	**Apache Software Foundation Apache 2.0.37-2.0.45; RedHat httpd-2.0.40-21.i386.rpm, 40-8.i386.rpm, httpd-devel-2.0.40-21.i386.rpm, 2.0.40-8.i386.rpm, httpd-manual-2.0.40-21.i386.rpm, 2.0.40-8.i386.rpm, mod_ssl-2.0.40-21.i386.rpm, 2.0.40-8.i386.rpm**	**A vulnerability exists in the 'apr_password_validate()' function due to improper use of specific thread-safe functions, which could let a remote malicious user cause a Denial of Service.**	**Apache:** http://www.apache.org/dist/httpd/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **RedHat:** ftp://updates.redhat.com/ ***YellowDog:*** ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/ ***Conectiva:*** ftp://atualizacoes.conectiva.com.br/9/	**Apache Basic Authentication Module Denial of Service** **CVE Name: CAN-2003-0189**	**Low**	**Bug discussed in newsgroups and websites.** **Vulnerability has appeared in the press and other public media.**
Multiple Vendors [92, 93] *Mandrake issued advisory*[94]	**Unix**	**GNU gzip 1.2.4 a, 1.2.4, 1.3, 1.3.2, 1.3.3, 1.3.5**	**A vulnerability exists in the 'znew' script due to a failure to securely handle temporary files, which could let a malicious user obtain elevated privileges.**	**OpenPKG:** ftp://ftp.openpkg.org/release/1.1/UPD/ **Debian:** http://security.debian.org/pool/updates/main/g/gzip/ ***Mandrake:*** http://www.mandrakesecure.net/en/ftp.php	**GZip ZNew Insecure Temporary File Creation** **CVE Name: CAN-2003-0367**	**Medium**	**Bug discussed in newsgroups and websites.**

[88] Red Hat Security Advisory, RHSA-2003:186-01, May 28, 2003.
[89] iDEFENSE Security Advisory, May 30, 2003.
[90] Yellow Dog Linux Security Announcement, YDU-20030603-1, June 3, 2003.
[91] Conectiva Linux Security Announcement, CLA-2003:661, June 16, 2003.
[92] Debian Security Advisory, DSA 308-1, June 7, 2003.
[93] OpenPKG Security Advisory, OpenPKG-SA-2003.031, June 11, 2003.
[94] Mandrake Linux Security Update Advisory, MDKSA-2003:068, June 16, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [95, 96] ***Mandrake issues update***[97]	**Unix**	**GNU gzip 1.2.4 a, 1.2.4, 1.3, 1.3.2, 1.3.3, 1.3.5**	**A vulnerability exists in the 'znew' script due to a failure to securely handle temporary files, which could let a malicious user obtain elevated privileges.**	**OpenPKG:** **ftp://ftp.openpkg.org/release/1.1/UPD/** **Debian:** **http://security.debian.org/pool/updates/main/g/gzip/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php**	**GZip ZNew Insecure Temporary File Creation** **CVE Name: CAN-2003-0367**	**Medium**	**Bug discussed in newsgroups and websites.**
Multiple Vendors[98] [99, 100] ***More advisories issued***[101, 102]	**Multiple**	**Apache Software Foundation Apache 2.0.37-2.0.45; RedHat httpd-2.0.40-21.i386.rpm, 40-8.i386.rpm, httpd-devel-2.0.40-21.i386.rpm, 2.0.40-8.i386.rpm, httpd-manual-2.0.40-21.i386.rpm, 2.0.40-8.i386.rpm, mod_ssl-2.0.40-21.i386.rpm, 2.0.40-8.i386.rpm**	**A vulnerability exists in the 'apr_psprintf()' Apache Portable Runtime (APR) library, which could let a remote malicious user execute arbitrary code.**	**Apache:** **http://www.apache.org/dist/httpd/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **RedHat:** **ftp://updates.redhat.com/** ***Apple:*** **http://docs.info.apple.com/article.html?artnum=61798** ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br/9/**	**Apache APR_PSPrintf Memory Corruption** **CVE Name: CAN-2003-0245**	**High**	**Bug discussed in newsgroups and websites.** **Vulnerability has appeared in the press and other public media.**

[95] Debian Security Advisory, DSA 308-1, June 7, 2003.
[96] OpenPKG Security Advisory, OpenPKG-SA-2003.031, June 11, 2003.
[97] Mandrake Linux Security Update Advisory, MDKSA-2003:068, June 16, 2003.
[98] Red Hat Security Advisory, RHSA-2003:186-01, May 28, 2003.
[99] iDEFENSE Security Advisory, May 30, 2003.
[100] Mandrake Linux Security Update Advisory, MDKSA-2003:063, May 30, 2003.
[101] Apple Security Updates, June 16, 2003.
[102] Conectiva Linux Security Announcement, CLA-2003:661, June 16, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[103, 104,] ***RedHat issues another advisory***[105]	**Unix**	**Linux kernel 2.4.0-test1-test12, 2.4-2.4.20**	**A remote Denial of Service vulnerability exists because some types of network traffic are not properly handled.**	**Debian:** **http://security.debian.org/ pool/updates/main/k/** **RedHat:** **ftp://updates.redhat.com/**	**Linux Kernel Excessive Traffic Remote Denial of Service** **CVE Name: CAN-2003-0364**	**Low**	**Bug discussed in newsgroups and websites.**
Multiple Vendors[106, 107,] ***RedHat issues another advisory***[108]	**Unix**	**Linux kernel 2.4.0-test1-test12, 2.4-2.4.20**	**A remote Denial of Service vulnerability exists because some types of network traffic are not properly handled.**	**Debian:** **http://security.debian.org/ pool/updates/main/k/** **RedHat:** **ftp://updates.redhat.com/**	**Linux Kernel Excessive Traffic Remote Denial of Service** **CVE Name: CAN-2003-0364**	**Low**	**Bug discussed in newsgroups and websites.**
Multiple Vendors[109, 110, 111] ***More advisories issued***[112]	**Unix**	**Linux kernel 2.0-2.0.39, 2.1, 2.1.89, 2.2-2.2.25, 2.3, 2.3.99, 2.3.99 pre1-pre7, 2.3.99, 2.4.0-test1-test12, 2.4-2.4.21 pre4, 2.5.0-2.5.69; RedHat Linux 7.1, i386, i586, i686, 7.2, athlon, i386, i586, i686, 7.3, i386, i686, 8.0, i386, i686, 9.0 i386**	**A Denial of Service vulnerability exists in the TTY layer.**	**Debian:** **http://security.debian.org/ pool/updates/main/k/** **Mandrake:** **ftp://ftp.planetmirror.com/ pub/Mandrake/updates/9.1 /RPMS/** **RedHat:** **ftp://updates.redhat.com/**	**Linux TTY Layer Denial of Service** **CVE Name: CAN-2003-0247**	**Low**	**Bug discussed in newsgroups and websites.**

[103] Red Hat Security Advisory, RHSA-2003:187-01, June 3, 2003.
[104] Debian Security Advisories, DSA 311-1 & 312-1, June 9, 2003.
[105] Red Hat Security Advisory, RHSA-2003:195-06, June 19, 2003.
[106] Red Hat Security Advisory, RHSA-2003:187-01, June 3, 2003.
[107] Debian Security Advisories, DSA 311-1 & 312-1, June 9, 2003.
[108] Red Hat Security Advisory, RHSA-2003:195-06, June 19, 2003.
[109] Red Hat Security Advisory, RHSA-2003:187-01, June 3, 2003.
[110] Debian Security Advisories, DSA 311-1 & 312-1, June 9, 2003.
[111] Mandrake Linux Security Update Advisory, MDKSA-2003:066, June 11, 2003.
[112] Debian Security Advisories, DSA 332-1 & 336-1, June 27 & 29, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts

Multiple Vendors[113, 114, 115]	Unix	Adobe Acrobat Reader (UNIX) 5.0 6;
		RedHat Linux 7.1, 7.2 ia64, i386, 7.3 i386, 8.0 i386, 9.0 i386;
		Xpdf Xpdf 0.92, 1.0, 1.0 1, 2.0, 2.0.1
			A vulnerability exists when hyperlinks have been enabled within the PDF viewer, which could let a remote malicious user execute arbitrary shell commands.	**YellowDog:**
				ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/ppc/
				RedHat:
				ftp://updates.redhat.com/
					Multiple Vendor PDF Hyperlinks	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

Multiple Vendors[116, 117, 118] ***More advisories issued***[119], [120]	**Unix**	**Linux kernel 2.4.0-test1-test12, 2.4-2.4.20, 2.4.21 pre1&pre4**	**A vulnerability exists in the MXCSR handler code due to a failure to handle malformed address data.**	**Debian:** **http://security.debian.org/pool/updates/main/k/** **Mandrake:** **ftp://ftp.planetmirror.com/pub/Mandrake/updates/9.1/RPMS/** **RedHat:** **ftp://updates.redhat.com/**	**Linux Kernel MXCSR Handler Malformed Address** **CVE Name: CAN-2003-0248**	**Low**	**Bug discussed in newsgroups and websites.**
myServer[121]	Windows	myServer 0.4.1	A Directory Traversal vulnerability exists which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	MyServer HTTP Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
myServer[122]	Windows, Unix	myServer 0.4.1	A Denial of Service vulnerability exists because the server does not properly handle certain invalid connections.	No workaround or patch available at time of publishing.	myServer Signal Handling Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
myServer[123]	Windows, Unix	myServer 0.4.1	A remote Denial of Service vulnerability exists due to insufficient bounds checking on arguments that are supplied via malicious HTTP GET requests.	No workaround or patch available at time of publishing.	MyServer Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[113] Red Hat Security Advisory, RHSA-2003:196-01, June 18, 2003.
[114] Yellow Dog Linux Security Announcement, YDU-20030620-1, June 20, 2003.
[115] Turbolinux Security Advisory, TLSA-2003-39, June 24, 2003.
[116] Red Hat Security Advisory, RHSA-2003:187-01, June 3, 2003.
[117] Debian Security Advisories, DSA 311-1 & 312-1, June 9, 2003.
[118] Mandrake Linux Security Update Advisory, MDKSA-2003:066, June 11, 2003.
[119] Red Hat Security Advisory, RHSA-2003:195-06, June 19, 2003.
[120] Debian Security Advisory DSA 332-1 & 336-1, June 27 & 29, 2003.
[121] Secunia Security Advisory, June 16, 2003.
[122] SecurityFocus, June 14, 2003.
[123] Securiteam, June 24,2 003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
MySQL AB[124]	Unix	MySQL 4.0.0-4.0.13	A buffer overflow vulnerability exists in the mysql_real_connect() function due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	MySQL mysql_real_ connect() Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
NANOG [125]	Unix	Traceroute 6.1.1	A vulnerability exists when certain 'max_ttl' and 'nprobe' values are processed, which could let a malicious user corrupt memory.	No workaround or patch available at time of publishing.	Traceroute-Nanog Integer Overflow	Medium	Bug discussed in newsgroups and websites.
Nethack [126] ***Patch & upgrade available*** [127] ***Debian issues advisories*** [128]	**Unix**	**Nethack 3.4 .0**	**A buffer overflow vulnerability exists when a specially crafted command string is submitted to the Nethack binary, which could let a malicious user execute arbitrary code.**	***Patch available at:*** **http://nethack.sourceforge.net/v340/bugmore/secpatch.txt** ***Upgrade available at:*** **http://nethack.sourceforge.net/v341/downloads.html** ***Debian:*** **http://security.debian.org/pool/updates/main/j/jnethack/**	**Nethack Local Buffer Overflow** **CVE Name: CAN-2003-0358**	**High**	**Bug discussed in newsgroups and websites. Exploit scripts have been published.**
NetScreen [129]	Multiple	ScreenOS 3.0.1, r1& r2, 3.0.2, 3.0.3, r1.1, 4.0, 4.0 – DIAL, 4.0.1, 4.0.2	A vulnerability exists because authentication can be bypassed, which could let an unauthenticated malicious user obtain access.	No workaround or patch available at time of publishing.	ScreenOS Unauthorized Access	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Next Generation Count [130]	Windows	Active FTPServer 2002 2.40	Several remote Denial of Service vulnerabilities exist when a malicious user submits excessive input via FTP commands such as 'USER,' 'cwd,' 'ls,' 'get,' or 'mkdir.'	The vendor will reportedly release a fixed version of the software in August 2003. Users should contact the vendor for further details.	FTPServer 2002 FTP Command Multiple Denial of Service	Low	Bug discussed in newsgroups and websites.
Nik Reiman[131]	Unix	Portmon 0.1-1.7	Several vulnerabilities exist: a vulnerability exists because certain files are not handled properly, which could let a malicious user obtain sensitive information.; and a Denial of Service vulnerability exists writing to files is not properly handled.	No workaround or patch available at time of publishing.	Portmon Information Disclosure & Denial of Service	Low/ Medium (Medium if sensitive information can be obtained)	Bug discussed in newsgroups and websites. There is no exploit code required.

[124] SCAN Associates Sdn Bhd Security Advisory, June 12, 2003.
[125] Bugtraq, June 20, 2003.
[126] Bugtraq, February 8, 2003.
[127] Bugtraq, March 1, 2003.
[128] Debian Security Advisories, DSA 316-1, 316-2, 316-3, June 12 & 17, 2003.
[129] Bugtraq, June 25, 2003.
[130] Secunia Security Advisory, June 13, 2003.
[131] Securiteam, June 18, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Norman Ramsey[132]	Unix	Noweb 2.9a	A vulnerability exists in the 'noroff' script due to insecure creation of temporary files, which could let a malicious user corrupt sensitive arbitrary files.	**Debian:** http://security.debian.org/pool/updates/main/n/noweb/	Noweb/Noroff Insecure Temporary File Creation CVE Name: CAN-2003-0381	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
NTA Monitor Ltd. [133]	Windows, Unix	ike-scan 1.0, 1.1	A vulnerability exists in the err_print() function when making a syslog() call, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.nta-monitor.com/ike-scan/download.htm	IKE-Scan Local Logging Format String	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Nuked Web[134]	Windows, Unix	GuestBook Host	Cross-Site Scripting vulnerabilities exists in the 'Name,' 'Email' or 'Message' fields due to insufficient sanitization of user-supplied data, which could let a malicious user execute arbitrary HTML code.	No workaround or patch available at time of publishing.	GuestBook Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Orville-Write[135]	Unix	Orville-Write 2.53	Multiple buffer overflow vulnerabilities exist due to a boundary error in the handling of multiple environment variables (e.g. "HOME"), which could let a malicious user execute arbitrary and possibly obtain root access.	Upgrades available at: http://www.unixpapa.com/software/orville-write-2.54.tar.gz **Debian:** http://security.debian.org/pool/updates/main/o/orville-write/	Orville-Write Multiple Buffer Overflows CVE Name: CAN-2003-0441	**High**	Bug discussed in newsgroups and websites.
osh[136]	Unix	osh 1.7	Several vulnerabilities exist: a buffer overflow vulnerability exists when processing environment variables, which could let a malicious user execute arbitrary code; and a buffer overflow vulnerability exists when redirection commands are processed, which could let a malicious user execute arbitrary code.	Upgrades available at: http://security.debian.org/pool/updates/main/o/osh/	osh Buffer Overflows	**High**	Bug discussed in newsgroups and websites.
phpBB Group[137]	Windows, Unix	phpBB 2.0.0-2.0.4	A vulnerability exists in the 'theme_info.cfg' script, which could let a malicious user obtain sensitive information or execute arbitrary commands.	No workaround or patch available at time of publishing.	PHPBB Theme_Info. CFG File Include	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit script has been published.

[132] Debian Security Advisory, DSA 323-1, June 16, 2003.
[133] Secure Network Operations, Inc. Advisory, SRT2003-06-12-0853, June 13, 2003.
[134] SecurityTracker Alert ID, 1007045,June 24, 2003.
[135] Debian Security Advisory, DSA 326-1, June 19, 2003.
[136] Debian Security Advisory, DSA 329-1, June 20, 2003.
[137] SecurityFocus, June 16, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
phpBB Group[138]	Windows, Unix	phpBB 2.0.4, 2.0.5	A Cross-Site Scripting vulnerability exists in the 'viewtopic.php' script due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain sensitive information.	**Workaround:** A temporary fix is available at: http://www.phpbb.com/phpBB/viewtopic.php?t=112052	phpBB Viewtopic.PHP Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
phpMy Admin[139]	Windows, Unix	phpMy Admin 2.0-2.0.5, 2.1-2.2.6, 2.3.1, 2.3.2, 2.4.0, 2.5.0, 2.5.1	Multiple vulnerabilities exist: Several Cross-Site Scripting vulnerabilities exist due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code; a Directory Traversal vulnerability exists due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain sensitive information; a path disclosure vulnerability exists, which could let a remote malicious user obtain sensitive information; and a vulnerability exists because passwords are stored in a plaintext format, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PHPMyAdmin Multiple Cross-Site Scripting	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required for the Cross-Site Scripting, path disclosure, & plaintext password vulnerabilities. Proof of Concept exploit has been published for the Directory Traversal vulnerability.
PMachine[140]	Windows, Unix	PMachine 2.2.1	A vulnerability exists in the 'pm/inc.lib.php' script due to insufficient verification before it is used in 'include' statements, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PMachine Lib.Inc.PHP Script	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
PMachine[141]	Windows, Unix	PMachine 1.0, 2.0-2.2.1	Several vulnerabilities exist: a vulnerability exists in the 'search/index.php' script because the 'keywords' parameter is improperly verified, which could let a remote malicious user execute arbitrary code; and a path disclosure vulnerability exists when various scripts are accessed, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	pMachine 'search/index. php'	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required however Proof of Concept exploits have been published.

[138] Bugtraq, June 19, 2003.
[139] Advisory: NSRG-15-7, June 18, 2003.
[140] Secunia Security Advisory, June 16, 2003.
[141] Securiteam, June 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PostNuke Development Team[142]	Windows, Unix	PostNuke Phoenix 0.723	Multiple Cross-Site Scripting vulnerabilities exists because the 'modules.php' script does not sufficiently sanitize data supplied via URI parameters, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	PostNuke 'Modules.PHP' Multiple Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
ProFTPD Project[143]	Unix	ProFTPD 1.2 pre1-pre11, 1.2.0rc1-1.2.0rc3, 1.2-1.2.9 rc1	A vulnerability exists in versions that that use the mod_sql module to manipulate PostgreSQL databases due to insufficient sanitization of user-supplied data when logging onto the server, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	ProFTPD 'mod_sql' Module	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Progress Software Corporation[144]	Windows NT 4.0/2000, Unix	4GL Compiler 9.1 D06	A buffer overflow vulnerability exists in the definition of datatypes when compiling '.p' files, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	4GL Compiler Datatype Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Progress Software Corporation [145]	Windows NT 4.0/2000, Unix	Progress Database 9.1, 9.1 B, 9.1 C , 9.1 D, D05, D06	A vulnerability exists in the '_dbagent' binary due to improper handling of untrusted input in some command line arguments, which could let a malicious user execute arbitrary code with root privileges.	No workaround or patch available at time of publishing.	Progress Database DBAgent	**High**	Bug discussed in newsgroups and websites.
Progress Software Corporation [146]	Windows NT 4.0/2000, Unix	Progress Database 9.1, 9.1 B, 9.1 C , 9.1 D, D05, D06	A vulnerability exists in the dlopen() function because untrusted input is not properly handled when opening shared libraries, which could let a malicious user execute arbitrary code with root privileges.	No workaround or patch available at time of publishing.	Progress Database dlopen() Function	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Proxomitron[147]	Multiple	Proxomitron	A remote Denial of Service vulnerability exists because some string types are not handled properly.	No workaround or patch available at time of publishing.	Proxomitron Remote Denial o Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required how a Proof of Concept exploit has been published.

[142] Bugtraq, June 13, 2003.
[143] Securiteam, June 19, 2003.
[144] Secure Network Operations, Inc. Advisory, SRT2003-06-20-1232, June 20, 2003.
[145] Secure Network Operations, Inc. Advisory, SRT2003-06-13-1009, June 14, 2003.
[146] Secure Network Operations, Inc. Advisory, SRT2003-06-13-0945, June 14, 2003.
[147] SecurityFocus, June 18, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Psunami Bulletin Board[148] ***Exploit scripts have been published.***[149]	**Multiple**	**Psunami Bulletin Board 0.2, 0.2.1, 0.3, 0.3.1, 0.4, 0.5, 0.5.1, 0.5.2**	**A vulnerability exists in query string parameters due to insufficient sanitization of shell metacharacters, which could let a remote malicious user execute arbitrary code.**	**No workaround or patch available at time of publishing.**	**Psunami Bulletin Board Psunami.CGI Remote Command Execution**	**High**	**Bug discussed in newsgroups and websites. Exploit has been published.**
QNX Software Systems Ltd.[150]	QNX	Demodisk 4.0	A Directory Traversal vulnerability exists due to improper validation of URLs, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	QNX Demo Web Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Remi Lefebvre[151]	Multiple	atftp 0.7cvs	Several vulnerabilities exist: a buffer overflow vulnerability exists in the command line parameter (-t) for 'timeout' due to insufficient bounds checking, which could let a malicious user execute arbitrary code; and a buffer overflow vulnerability exists in the command line parameter (-b) for 'blocksize' due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	ATFTP Timeout Command Line Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published for the timeout buffer overflow.
RSA Security[152]	Windows	ACE/Agent for Web 5.0, ACE/Agent for Windows 5.0	A Cross-Site Scripting vulnerability exists because certain characters are not properly escaped from user-supplied input before generating a page that contains the user's input, which could let a remote malicious user execute arbitrary HTML and script code.	Upgrades available at: ftp://ftp.rsasecurity.com/support/Patches/Ace/Agent/	RSA SecurID ACE Agent Cross-Site Scripting CVE Name: CAN-2003-0389	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Sambar Technol-ogies[153]	Windows 95/98/ME/ NT 4.0/2000	Sambar Server 4.1, 4.2.1, 4.3, & 4.4 production, 4.3, 4.4 Beta 3, 5.0 beta1-beta6, 5.1	A remote Denial of Service vulnerability exists in the 'search.pl' component when a malicious user submits a specially crafted query via a POST request.	No workaround or patch available at time of publishing.	Sambar Server 'search.pl' Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[148] SecurityFocus, January 14, 2003.
[149] SecurityFocus, June 17, 2003.
[150] Bugtraq, June 22, 2003.
[151] SecurityFocus, June 13, 2003.
[152] Rapid7, Inc. Security Advisory, R7-0014, June 18, 2003.
[153] SecurityTracker Alert ID, 1007016, June 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Schmolze Studios[154]	Unix	sdfingerd 1.1	A vulnerability exists because group privileges are not dropped before commands are executed in the user '.plan' files, which could let a malicious user obtain root privileges.	No workaround or patch available at time of publishing.	SDFingerD Root Privileges	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
SGI[155]	Unix	IRIX 6.5.19, 6.5.20	Several vulnerabilities exist: a Denial of Service vulnerability exists when inet handles network-based scans; and a vulnerability exists in the X snoop network protocol analyzer, which could let a malicious user obtain elevated privileges.	Patches available at: ftp://patches.sgi.com/support/free/security/patches/	IRIX IPV6 InetD Scan Denial of Service & Snoop	Low/ Medium (Medium if elevated privileges can be obtained)	Bug discussed in newsgroups and websites. Denial of Service vulnerability may be exploited using a network scanning utility
Sharp Zaurus[156]	Windows, Unix	Sharp Zaurus SL-5500, 3.1 ROM, SL-600	A vulnerability exists for the Samba server when mounting the device to the docking station, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Sharp Zaurus Samba Server Unauthorized Remote Filesystem Access	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
silent Thought Software[157]	Windows NT 4.0	Simple Web Server 1.0	A Directory Traversal vulnerability exists due to insufficient sanitization of web requests, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Simple Web Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Snitz Forums 2000[158]	Windows, Unix	Snitz Forums 2000 3.4 .03	Several vulnerabilities exist: a Cross-Site Scripting vulnerability exists in the 'search.asp' script due to insufficient santization of data, which could let a malicious user execute arbitrary code; a vulnerability exists because the authentication cookie of another user can be retrieved, which could let a remote malicious user bypass authentication and obtain unauthorized access; and a vulnerability exists when a forgotten password is requested, which could let a malicious user reset arbitrary account passwords.	No workaround or patch available at time of publishing.	Snitz Forums Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published for the Cross-Site Scripting vulnerability. There is no exploit code required for the authentication bypass and password reset vulnerabilities.

[154] Secunia Security Advisory, June 23, 2003.
[155] SGI Security Advisory, 20030607-01-P, June 24, 2003.
[156] Bugtraq, June 24, 2003.
[157] Securiteam, June 12, 2003.
[158] Bugtraq, June 16, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sphera[159]	Windows, Unix	Hosting Director 1.0, 2.0, 3.0	Multiple vulnerabilities exist: several buffer overflow vulnerabilities exist due to insufficient bounds checking when copying user-supplied data into reserved memory space, which could let a remote malicious user cause a Denial of Service; a vulnerability exists in the VDS Control Panel because the authentication system can be bypassed, which could let a remote malicious user make arbitrary account configuration modifications; multiple Cross-Site Scripting vulnerabilities exist in the 'login_screen.php' and 'sm_login_screen.php' scripts, which could let a remote malicious user execute arbitrary code; and a vulnerability exists due to a weak method of generating session IDs, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Hosting Director Multiple Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Sun Micro-systems, Inc.[160]	Unix	SunMC 2.1.1, 3.0, 3.0RR	A vulnerability exists due to weak permissions on created directories and files, which could let a malicious user modify arbitrary files.	Patches available at: http://sunsolve.sun.com	Sun Management Center Insecure File Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Sun Micro-systems, Inc.[161]	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86	Buffer overflow vulnerabilities exists in the dbm_open(), ndbm(), dbm(), and dbminit() library functions due to insufficient bounds checking when external supplied data is copied into an internal memory buffer, which could let a malicious user obtain unauthorized root access.	Patches available at: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F55420	Multiple Sun Buffer Overflows	**High**	Bug discussed in newsgroups and websites.

[159] Bugtraq, June 13, 2003.
[160] Sun(sm) Alert Notification, 55141, June 16, 2003.
[161] Sun Alert ID, 55420, June 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Surf Control[162]	Windows 2000	SurfControl Web Filter for Microsoft ISA Server 4.2.0.1, SurfControl Web Filter for Windows NT/2000 4.2 .0.1	A Directory Traversal vulnerability exists due to insufficient sanitization, which could let a malicious user obtain sensitive information.	**Workaround:** Disable the reports server by going to "Admin Tools" -> "Services" and stopping the SurfControl Web Filter Report Server.	SurfControl Web Filter Directory Traversal	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Symantec [163]	Windows	RuFSI Utility Class	A buffer overflow vulnerability exists because the 'CompareVersionStrings' function doesn't verify input properly, which could let a remote malicious user execute arbitrary code.	Symantec advises users who have recently visited Symantec Security Check to re-run a new Security Scan. This will cause the previous ActiveX control to be replaced with one that is not vulnerable to this issue.	Symantec RuFSI ActiveX Control Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. Vulnerability has appeared in the press and other public media.
Tarantella Inc. [164]	Unix	Enterprise 3 3.0, 3.0 1, 3.10, 3.11, 3.20, 3.30	A vulnerability exists because a user's keypresses can be sent to another user's emulator session, which could let a malicious user obtain sensitive information.	**Workaround:** Administrators are advised to issue the following command to ensure the configuration setting is set to 1. /opt/tarantella/bin/tarantella config edit --xpe-maxusers 1 --cpe-maxusers 1	Enterprise Redirected Keypress	Medium	Bug discussed in newsgroups and websites.
tcptrace route[165]	Unix	tcptrace route 1.2	A vulnerability exists because all root privileges are not relinquished after obtaining a file descriptor, which could let a malicious user obtain elevated privileges.	**Debian:** http://security.debian.org/pool/updates/main/t/tcptraceroute/	tcptraceroute Failure To Relinquish Root CVE Name: CAN-2003-0489	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Tmax Soft Co., Ltd [166]	Windows, Unix	JEUS 3.1.4 p1	A Cross-Site Scripting vulnerability exists in the 'url.jsp' script due to insufficient filtering of user-supplied input, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.tmax.co.kr	JEUS Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[162] Bugtraq, June 19, 2003.
[163] Security Advisory, CC060304, June 23, 2003.
[164] Tarantella Security Bulletin #07, June 13, 2003.
[165] Debian Security Advisory, DSA 330-1, June 23, 2003.
[166] STG Security Advisory, June 17, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Tom Hombergs[167]	Windows, Unix	pod.board 1.1	Several vulnerabilities exist: a vulnerability exists in the 'forum_details.php' script due to insufficient sanitization of data supplied via URI parameters and input fields, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists in the 'new_topic.php' script due to insufficient sanitization sanitization of data supplied via URI parameters and input fields, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Pod.Board 'Forum_ Details.PHP' & 'New_Topic. php'	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Tutos[168]	Unix	Tutos 1.1	Multiple vulnerabilities exist: a Cross-Site Scripting vulnerability exists in the 'file_select' script due to insufficient filtering of HTML, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the 'file_new' script, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Tutos Multiple Vulnerabilities	High	Bug discussed in newsgroups and websites. There is no exploit code required however a Proof of Concept exploits have been published.
Vignette[169] ***Upgrade information issued***[170]	**Unix**	**Content Suite V7, V6, StoryServer 4.0, 4.1, 5.0, 6.0**	**A vulnerability exists due to a flaw in the way the size of certain characters in URI variables are calculated, which could let a remote malicious user obtain sensitive information.**	***The vendor has posted a response to this issue at the following location:*** **http://support.vignette.com/VOLSS/KB/View/1,,5557,00.html**	**Vignette Memory Disclosure** **CVE Name: CAN-2003-0400**	**Medium**	**Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.**
Vignette[171] ***Upgrade information issued***[172]	**Windows NT 4.0/2000, Unix**	**Content Suite V5-V7, StoryServer 4.0, 4.1, 5.0, 6.0**	**Multiple Cross-Site Scripting vulnerabilities exist due to insufficient sanitization of HTML characters from user-supplied data, which could let a malicious user execute arbitrary HTML and script code.**	***This vulnerability does not affect Vignette Platform releases 6.0.4 and later. The vendor has stated that there are EFIXes available for vulnerable versions of the Vignette CMS. Affected users are advised to open a VOLSS ticket for further details or to request an EFIX.***	**Multiple Vignette Cross-Site Scripting Vulnerabilities** **CVE Name: CAN-2003-0404**	**High**	**Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.**

[167] SecurityTracker Alert ID, 1006990, June 14, 2003.
[168] Kereval Security Advisory, KSA-001, June 23, 2003.
[169] S21SEC Advisory, S21SEC-018, May 26, 2003.
[170] SecurityFocus, June 17, 2003.
[171] S21SEC Advisory, S21SEC-023, May 26, 2003.
[172] SecurityFocus, June 17, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Vignette[173] *Upgrade information issued*[174]	Windows NT 4.0/2000, Unix	Content Suite V5-V7, StoryServer 4.0, 4.1, 5.0, 6.0	A vulnerability exists in the 'NEEDS' and 'VALID_PATHS commands, which could let a remote malicious user execute arbitrary code.	*This vulnerability does not affect Vignette Platform releases 6.0.4 and later. The vendor has stated that there are EFIXes available for vulnerable versions of the Vignette CMS. Affected users are advised to open a VOLSS ticket for further details or to request an EFIX.*	Vignette NEEDS Command CVE Name: CAN-2003-0405	High	Bug discussed in newsgroups and websites.
Vignette[175] *Upgrade information issued*[176]	Windows NT 4.0/2000, Unix	Content Suite V5-V7, StoryServer 4.0, 4.1, 5.0, 6.0	A vulnerability exists in the login template, which could let a remote malicious user obtain sensitive information.	*The vendor has posted a response to this issue at the following location:* http://support.vignette.com/VOLSS/KB/View/1,,5557,00.html	Vignette Login Template Information Leakage CVE Name: CAN-2003-0402	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Vignette[177] *Upgrade information issued*[178]	Windows NT 4.0/2000, Unix	Content Suite V5-V7, StoryServer 4.0, 4.1, 5.0, 6.0	A vulnerability exists because several templates are installed in the /vgn directory, which could let a remote malicious user obtain sensitive information.	*The vendor has posted a response to this issue at the following location:* http://support.vignette.com/VOLSS/KB/View/1,,5557,00.html	Vignette Template Information Leakage CVE Name: CAN-2003-0401	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Vignette[179] *Upgrade information issued*[180]	Windows NT 4.0/2000, Unix	Content Suite V5-V7, StoryServer 4.0, 4.1, 5.0, 6.0	A remote Denial of Service vulnerability exists because several templates are installed in the /vgn directory.	*The vendor has posted a response to this issue at the following location:* http://support.vignette.com/VOLSS/KB/View/1,,5557,00.html	Vignette Template Remote Denial of Service CVE Name: CAN-2003-0403	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Vignette[181] *Upgrade information issued*[182]	Windows NT 4.0/2000, Unix	Content Suite V7, V6, StoryServer 4.0, 4.1, 5.0, 6.0	A vulnerability exists which could let a remote malicious user execute arbitrary commands.	*The vendor has posted a response to this issue at the following location:* http://support.vignette.com/VOLSS/KB/View/1,,5557,00.html	Vignette SSI Injection CVE Name: CAN-2003-0398	High	Bug discussed in newsgroups and websites. There is no exploit code required.

[173] S 2 1 S E C Advisory, S21SEC-024, May 26, 2003.
[174] SecurityFocus, June 17, 2003.
[175] S 2 1 S E C Advisory, S21SEC-020, May 26, 2003.
[176] SecurityFocus, June 17, 2003.
[177] S 2 1 S E C Advisory, S21SEC-019, May 26, 2003.
[178] SecurityFocus, June 17, 2003.
[179] S 2 1 S E C Advisory, S21SEC-020, May 21, 2003.
[180] SecurityFocus, June 17, 2003.
[181] S 2 1 S E C Advisory, S21SEC-016, May 26, 2003.
[182] SecurityFocus, June 17, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Vignette[183] ***Upgrade information issued***[184]	**Windows NT 4.0/2000, Unix**	**Content Suite V7, V6, StoryServer 4.0, 4.1, 5.0, 6.0**	**A vulnerability exists in the Legacy Tool application due to insufficient access restrictions, which could let an unauthorized remote malicious user execute database queries.**	***The vendor has posted a response to this issue at the following location:*** **http://support.vignette.com/VOLSS/KB/View/1,,5557,00.html**	**Vignette Unauthorized Legacy Tool Access** **CVE Name: CAN-2003-0399**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
Webcam Now[185]	Multiple	Webcam Now	A vulnerability exists because usernames and passwords are stored in a plaintext format, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	WebcamNow Plaintext Password Storage	Medium	Bug discussed in newsgroups and websites. There is no exploit code required. Vulnerability has appeared in the press and other public media.
WebFS[186]	Unix	WebFS 1.17, 1.18	A buffer overflow vulnerability exists due to insufficient bounds checking on overly long Request-URI HTTP requests, which could let a remote malicious user execute arbitrary code.	Upgrades available at: http://bytesex.org/misc/webfs_1.19.tar.gz **Debian:** http://security.debian.org/pool/updates/main/w/webfs/	WebFS Request-URI Buffer Overflow CVE Name: CAN-2003-0445	**High**	Bug discussed in newsgroups and websites.
WebJeff[187]	Multiple	File manager 1.6	Several vulnerabilities exist: a Directory Traversal vulnerability exists in the 'index.php3' file due to insufficient path verification, which could let a malicious user obtain sensitive information; and a vulnerability exists because authentication credentials are stored in plaintext, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Filemanager Directory Traversal & Authentication Storage	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published for the Directory Traversal vulnerability. There is no exploit code required for the authentication vulnerability.

[183] S 2 1 S E C Advisory, S21SEC-017, May 26, 2003.
[184] SecurityFocus, June 17, 2003.
[185] SecurityFocus, June 12, 2003.
[186] Debian Security Advisory, DSA 328-1, June 19, 2003.
[187] Secunia Security Advisory, June 25, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
XBlock Out [188]	Unix	xbl 1.0k, 1.0i	Several buffer overflow vulnerabilities exists due to boundary errors in the handling of command line arguments and the use of the 'XBLOPTIONS' environment variable, which could let a malicious user obtain elevated privileges and possibly execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/x/xbl/	XBlockOut XBL Multiple Buffer Overflow	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
XMB[189]	Windows, Unix	Forum 1.8, 1.8 SP1	Multiple Cross-Site Scripting and HTML injection vulnerabilities exist due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	XMB Forum Multiple Cross-Site Scripting And HTML Injection	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Xoops[190]	Windows, Unix	Xoops Tutorials Module 2.0	A vulnerability exists in the upload function due to insufficient verification of file type, which could let a remote malicious user execute arbitrary commands.	Upgrade available at: http://www.mytutorials.info/modules/mydownloads/	Xoops/ E-Xoops Tutorials Module Upload Function	**High**	Bug discussed in newsgroups and websites.
Zope[191]	Unix	Zope 2.5.1, 2.6.1	Multiple vulnerabilities exist: a path disclosure vulnerability exists when an upload operation is invoked and the target file does not exist as a URI parameter, which could let a remote malicious user obtain sensitive information; a vulnerability exists in the 'addItems' script when a value of excessive size is passed as a URI parameter, which could let a remote malicious user obtain sensitive information; a path disclosure vulnerability exists when an invalid query operation is invoked that uses Shopping Cart example scripts, which could let a remote malicious user obtain sensitive information; and a vulnerability exists in the 'ExampledbBrowseReport' example script due to insufficient input validation, which could let a remote malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Zope Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.

[188] Debian Security Advisory, DSA 327-1, June 19, 2003.
[189] Bugtraq, June 23, 2003.
[190] Bugtraq, June 16, 2003.
[191] Exploitlabs.com Advisory, EXPL-A-2003-009, June 19, 2003.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between June 13 and June 24, 2003, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 37 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	**Script name**	**Script Description**
June 24, 2003	**deadbeat.pl**	**Perl script that exploits the MyServer Remote Denial of Service vulnerability.**
June 24, 2003	DSR-geekrellm.pl	Perl script that exploits the Gkrellmd Remote Buffer Overflow vulnerability.
June 24, 2003	gkrellmcrash.pl	Perl script that exploits the Gkrellmd Remote Buffer Overflow vulnerability.
June 24, 2003	heap_off_by_one.txt	A short paper discussing exploitation of vulnerabilities consisting of a null byte written passed the end of a dynamically allocated buffer.
June 24, 2003	wa_dlexp.c	Script that exploits the WebAdmin USER Parameter Buffer Overflow vulnerability.
June 24, 2003	wa_exp.c	Script that exploits the WebAdmin USER Parameter Buffer Overflow vulnerability.
June 24, 2003	**xdune.c**	**Script that exploits the Dune Buffer Overflow vulnerability.**
June 24, 2003	**xlbs.c**	**Exploit for the LBreakOut2 Remote Format String vulnerability.**
June 23, 2003	**armidaDOS.c**	**Script that exploits the Armida Databased Web Server Remote Denial of Service vulnerability.**
June 23, 2003	**DSR-korean-elm.pl**	**Perl script that exploits the Elm Local TERM Environment Variable Buffer Overrun vulnerability.**

Date of Script (Reverse Chronological Order)	Script name	Script Description
June 23, 2003	snacktime.tgz	Remote OS fingerprinting tool written in Perl that analyzes the retransmission timeout lengths of a TCP handshake to detect remote operating systems.
June 23, 2003	**xsdfingerd.sh**	**Exploit for the SDFingerD Root Privileges vulnerability.**
June 22, 2003	svtun-1.2.tar.gz	A simple and powerful distributed sniffer which is based on virtual tunnels. It extends the basic encryption and compression functionality of vtun to support a new interface type "sniff" and provides simple and efficient packet filtering and basic assymetric processing for client/server roles.
June 21, 2003	**0x82-GNATS_own.c**	**Script that exploits the GNATS Buffer Overflows vulnerability.**
June 21, 2003	**0x82-GNATS_sux.c**	**Script that exploits the GNATS Environment Variable Buffer Overflow vulnerability.**
June 21, 2003	consroot.exp	This script is used to automate escalation of normal user privileges to root making use of FORTH hacking on Sparc hardware.
June 21, 2003	covert_paper.txt	Document that describes exploitation of data streams authorized by a network access control system for arbitrary data transfers: tunneling and covert channels over the HTTP protocol.
June 21, 2003	hack-nethack0x02.tar.gz	Exploit for the NetHack / Jnethack Incorrect Permissions vulnerability.
June 21, 2003	**mame_exp.c**	**Script that exploits the Xmane Buffer Overflow vulnerability.**
June 21, 2003	phpbb_sql.pl	Perl script that exploits the phpBB Viewtopic.PHP Cross-Site Scripting vulnerability.
June 20, 2003	**procex.c**	**Script that exploits the Linux /proc Filesystem Information Disclosure vulnerability.**
June 19, 2003	**0x36-assabuse.c**	**Script that exploits the Abuse-SDL Buffer Overflow vulnerability.**
June 19, 2003	**keriobaby.c**	**Script that exploits the MailServer Buffer Overflow vulnerabilities.**
June 19, 2003	**runlevel-proftpd.pl**	**Perl script that exploits the ProFTPD ‘mod_sql’ Module vulnerability.**
June 18, 2003	evil.tex.uu	Exploit for the Multiple Vendor PDF Hyperlinks vulnerability.
June 17, 2003	**cgi.psunami.pl**	**Script that exploits the Psunami Bulletin Board Psunami.CGI Remote Command Execution vulnerability.**
June 17, 2003	HappyMail.pl	Perl script that exploits the HappyMall E-Commerce Software Remote Arbitrary Command Execution vulnerability.
June 17, 2003	**Psunami.pl**	**Script that exploits the Psunami Bulletin Board Psunami.CGI Remote Command Execution vulnerability.**
June 17, 2003	**StockmanShop.pl**	**Script that exploits the Stockman Shopping Cart Arbitrary Command Execution vulnerability.**
June 16, 2003	amap-2.7.tar.gz	A scanning tool that allows you to identify the applications that are running on a specific port by connecting to the port(s) and sending trigger packets.
June 16, 2003	firepass-1.0.2a.tar.gz	A tunneling tool that bypasses firewall restrictions and encapsulates data flows inside of HTTP POST requests.
June 16, 2003	**mailtraq-password-ex.pl**	**Perl script that exploits the Mailtraq Weak Encoding vulnerability.**
June 16, 2003	**phpbbexp.c**	**Script that exploits the PHPBB Theme_Info. CFG File Include vulnerability.**

Date of Script (Reverse Chronological Order)	Script name	Script Description
June 14, 2003	cctt-0.1.7.tar.gz	"Covert Channel Tunneling Tool," is a tool that presents several exploitation techniques allowing the creation of arbitrary data transfer channels in the data streams (TCP, UDP, and HTTP) authorized by a network access control system.
June 14, 2003	linux-wb.c	Script that exploits the WebDAV ntdll.dll remote vulnerability.
June 13, 2003	ethereal-0.9.13.tar.gz	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
June 13, 2003	**expl-atftp.pl**	**Perl script that exploits the ATFTP Timeout Command Line Buffer Overflow vulnerability.**

Trends

- **The Fortnight Internet worm takes advantage of a the Microsoft VM ActiveX security vulnerability for which Microsoft released a security patch three years ago. When this security breach is left unpatched the worm's code is allowed to be executed on victim computers. For more information see entry in Virus Section.**
- **A growing trend sees spammers targeting home computers with Trojan programs to remotely send out spam. Spammers are less likely to crack corporate boxes and are now increasingly turning toward using large quantities of home computers.**
- **The Department of Homeland Security has noticed an increase in the use of mass mailing techniques to distribute malicious code. Several recent forms of malicious code, such as the W32/Fizzer@MM Worm (see DHS Advisory 03-#023), variations of the Sobig virus (W32/Sobig-A, B and C), and BugBear (W32/BugBear A and B) were propagated via e-mail. For more information see: http://www.nipc.gov/publications/infobulletins/2003/MassMailingMalicious%20Code.htm.**
- **The underlying code for the Slammer worm is planned to be published by *Wired* magazine. The article, which will be published in Wired's July issue due out on Tuesday, details how the Slammer worm, also known as "SQL Slammer," spread rapidly through the Internet on Jan. 25, shutting down Internet service providers in South Korea, disrupting plane schedules and knocking out automatic teller machines.**
- **A new version of the network worm "Sobig" has been detected, Sobig.c. There here have been numerous registered infections from the new version of this malicious program.**
- **Sobig.B (Aliases: Palyh or Mankx) infections have been reported from over 80 countries worldwide. This worm is spreading at an increasing pace. The largest infections seem to be in UK and USA. It spreads via e-mail attachments and Windows network shares. The e-mails sent by the worm pretend to come from support@microsoft.com and they contain the message text "All information is in the attached file." Windows users everywhere are urged to update their anti-virus definitions.**
- According to new research, nearly three-quarters of malicious connections to wireless networks are used for sending spam. A survey found that almost a quarter of unauthorized connections to the wireless LANs were intentional, and 71 per cent of those were used to send e-mails.
- **The Department of Homeland Security (DHS), Information Analysis and Infrastructure Protection (IAIP) has issued an advisory to heighten awareness of a recently discovered Snort(TM) vulnerability, a heap overflow in the Snort "stream4" preprocessor (CAN-2003-0029). For more information see 'Bugs, Holes, & Patches Table (CyberNotes 2003-08) and DHS/IAIP Advisory 03-018, located at: http://www.nipc.gov/warnings/advisories/2003/03-018.htm**
- **The number of security events detected by companies in the first quarter of 2003 jumped nearly 84 percent over the preceding three months. The increase in events, which can include minor probes for holes in network security as well as major attacks, stems mainly from an increase in worms and automated attack software.**

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

BAT.Snoital@mm (Batch File Worm): This is a batch file worm that will try to delete antivirus software from your computer. It spreads through MAPI-enabled e-mail clients, such as Microsoft Outlook and IRC. The e-mail will have the following characteristics:

- Subject: Free antivirus program
- Attachment: Nod32.bat

HLLP.Tivo.8784 (DOS Virus): This is a prepending, memory-resident DOS virus that infects all the .com and .exe files in drives C and D, and in the system path. The size of an infected file is increased by 8,784 bytes.

I-Worm.Mapson (Internet Worm): Mapson Internet worm spreads via the Internet attached to infected e-mails and through file sharing networks and folders. The worm itself is a Windows PE EXE file about 180K in size when compressed by UPX, the decompressed size is about 440K). It is written in Borland Delphi 6.0. While installing, the worm copies itself to the Windows system directory using the name Lorraine.exe. It them registers this file in the system registry auto-run key:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run Lorraine = %SystemDir%\Lorraine.exe

JS/Fortnight-D (Alias: JS.JJBlack) (JavaScript Worm): This virus has been reported in the wild. It a combination of JavaScripts and Java Applets. When an e-mail infected with JS/Fortnight-D is read by an HTML aware mail client, the virus attempts to open a website. The website runs a Java Applet that makes use of Troj/ByteVeri-A to run itself locally. JS/Fortnight-D then attempts to drop a file S.HTM in WINDOWS that it will set as the signature for Outlook Express 5.0. JS/Fortnight-D also creates a file in the Windows folder called hosts. The hosts file has the effect of subverting access to certain websites. JS/Fortnight-D edits the following registry entries:

- HKCU\Software\Microsoft\Internet Explorer\Main\Search Page
- HKCU\Software\Microsoft\Internet Explorer\Main\Search Bar
- HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel\SecurityTab
- HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel\AdvancedTab
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\URL\DefaultPrefix

The following files will be dropped in the Favorites Folder:

- Nude Nurses.url
- Search You Trust.url
- Your Favorite Porn Links.url

JS/Fortnight-D exploits a vulnerability in the Microsoft VM ActiveX component. If an affected web page is opened, a JScript embedded on the page attempts to use the vulnerability in order to drop files on a local drive, change registry keys without the user's knowledge or perform any other malicious action on the local computer. For more details about the Microsoft VM ActiveX component exception vulnerability please see Microsoft Security Bulletin MS00-075.

JS/Fortnight-E (JavaScript Worm): This is a virus that is combination of JavaScripts and Java Applets. When an e-mail infected with JS/Fortnight-E is read by an HTML aware mail client, the virus attempts to open a website. The website runs a Java Applet that makes use of Troj/ByteVeri-A to run itself locally. It then attempts to drop a file S.HTM in WINDOWS that it will set as the signature for Outlook Express 5.0. JS/Fortnight-E also creates a file in the Windows folder called hosts. The hosts file has the effect of subverting access to certain websites. JS/Fortnight-E edits the following registry entries:

- HKCU\Software\Microsoft\Internet Explorer\Main\Search Page
- HKCU\Software\Microsoft\Internet Explorer\Main\Search Bar
- HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel\SecurityTab
- HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel\AdvancedTab
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\URL\DefaultPrefix

The following files will be dropped in the Favorites Folder:

- Nude Nurses.url
- Search You Trust.url
- Your Favorite Porn Links.url

JS/Fortnight-E exploits a vulnerability in the Microsoft VM ActiveX component. If an affected web page is opened, a JScript embedded on the page attempts to use the vulnerability in order to drop files on a local drive, change registry keys without the user's knowledge or perform any other malicious action on the local computer.

JS/Fortnight-F (Alias: Trojan.JS.SetPage) (JavaScript Worm): This virus has been reported in the wild. It is a JScript encoded form of JS/Fortnight-D.

PE_NIMDA.L (Aliases: W32.Nimda.R, I-Worm.Nimda.h) (File Infector Virus): This file and network-infector lacks the functionality of previous NIMDA variants. Unlike its more successful predecessors, this variant has no mass-mailing capability and does not exploit all the vulnerabilities employed by previous variants. It infects all the local .EXE files that it finds in a certain registry key and .EXE files found in network-shared folders by attaching its malicious code at the start of the host file and appending a malicious .DLL file to the target file.

VBS.Butterhot (Aliases: VBS/Rettub, IRC-Wrom.Butterhot) (Visual Basic Script Worm): This is a Visual Basic Script (VBS) worm that attempts to send itself by mIRC. The existence of the file sex.vbs is an indication of a possible infection.

VBS.Pet_Tick.N (Aliases: VBS.Dilna-B, VBS.Dilan) (Visual Basic Script Virus): This is a Visual Basic Script (VBS) virus that infects HTML files. It creates the file, %Windir%\mylover.exe, and then modifies the registry so that this file executes upon start up. VBS.Pet_Tick.N appends itself to any HTML files in the \Windows, \My Documents, and \Internet Temporary Folder directories. With default security settings in Internet Explorer, acknowledge a security warning dialog box before the virus executes. When VBS.Pet_Tick.N is executed, it creates the file, %Windir%\Mylover.exe. This file is detected as W95.Pet_Tick.gen and adds the value, "Lover32"="%WINDIR%\mylover.exe," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that VBS.Pet_Tick.N runs when you start Windows. It iterates through the %Windir%, %System%, Temporary, My Documents, and Desktop Folders, searching for the files with the .HTM and .HMTL extensions. The virus also appends itself to these files. Due to a bug in the code, the virus will re-infect the files that have already been infected.

VBS.Pinprick@mm (Visual Basic Script Worm): This is a mass-mailing worm that infects the .htm and .vbs files. This worm requires a MAPI-compliant e-mail client, such as Microsoft Outlook, to propagate. The e-mail will have a variable subject name and an attachment named Winhtm32.html.

VBS/Suhd-A (Aliases: X97M.Suhd, VBS_DELTAD.B, W32/DeltaD@MM, I-Worm.Deltad) (Visual Basic Script Worm): This is an Internet worm which e-mails itself to every contact in the Microsoft Windows address book. The e-mails have the following characteristics:

- Subject line: FW: Daily Report!!!
- Attached file: Daily Report.Xls

If opened, Daily Report.Xls creates a file called suhdlog.vbs in the Windows folder. Suhdlog.vbs is the mailing component of the worm.

W32/Aplch.worm (Win32 Worm): This is an Internet worm that propagates via KaZaA and other peer-to-peer networks. When run, it displays message "Windows has caused an error and needs to restart" in a command window. It then attempts to reboot the machine. It creates the following directories:

- C:\windows\PCdir
- C:\windows\PCdir\Netlogs
- C:\windows\SYSTEM\sysdlls

It creates/modifies the following registry key to enable KaZaA file sharing:

- HKEY_CURRENT_USER\Software\Kazaa\LocalContent "dir0" = "012345:C:\WINDOWS\system\sysdlls"

The worm copies itself to the Startup folder as "PCB115.com" to load itself at Windows startup. It checks for other P2P network shares such as Morpheus, Edonkey2000, Gnucleus, ICQ, etc. If any share directory is found, it copies itself to the directory with various file names. The worm searches Windows and Windows temporary directory for files with the following extension: .txt, .js, .doc, .rtf, .pwl, .ini, and .log. It copies any files found to c:\windows\SYSTEM\sysdlls directory. So the files are visible over the network.

W32.Anirak (Win32 Virus): This is a virus that will copy itself to the floppy drive as Karina.exe or Shakira.exe. It will also modify the Autoexec.bat file to display a text message. When W32.Anirak is executed, it copies itself as the following files:

- C:\Windows\System\Winalx.bat
- C:\Windows\System\Runonce.com

and attempts to modify the file, C:\Autoexec.bat, to display a political message. Next is adds the value, "SystemR"="c:\windows\system\runonce.com," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the virus runs when you start Windows. The virus also adds the value, "SystemW"="c:\windows\system\winalx.bat," to the registry key:

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the virus runs when you start Windows. It attempts to copy itself to the floppy drive as the following files:

- A:\Karina.exe
- A:\Shakira.exe

W32/CornishAcid (Win32 Worm): This is an Internet worm that spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book. If executed, the worm searches for files with the .exe extension and replaces the original file with a copy of itself. The original file will then contain a .acid extension. It will then create a new text file in the \windows\ directory under the name "Cornishacid.txt.”

W32/Crock-A (Aliases: I-Worm.Crock, WORM_CROCK.A, Win32.Crock.A worm, W32.Danvee@mm) (Win32 Worm): This is a worm which spreads by e-mail. Infected e-mails contain an attachment named CROCK.EXE or CROCK.SCR. If you run this attachment, a dialog containing a Yahoo icon pops up, inviting you to "Connect to everything in Y!.” You are asked to type in your "Yahoo ID" (which is filled in with your computer name) and your "password,” and then to click [OK] or [Cancel]. If you click [OK], W32/Crock-A will e-mail itself to everyone in your address book, producing e-mails with the following characteristics:

- Subject line: Your free yahoo account and file!
- Message text:
  Yahoo ID: YOUR-PC-NAME
  password: the-password-you-typed-in

But if you click [Cancel], W32/Crock-A will produce an e-mail with these characteristics:

- Subject line: Yahoo Game House
- Message text:
  >From the makers of Yahoo Game House, here is a new game
  from vAndEEd0!

W32/Crock-A also creates a hidden copy of itself (using the name CROCK.EXE or CROCK.SCR) in your startup folder. This means that the worm relaunches itself every time you log on to your computer. It adds the following value to your registry:

- HKCU\Software\Microsoft\Windows\CurrentVersion\System Signature

If this registry value already exists when W32/Crock-A starts up, the worm will neither pop up its bogus Yahoo dialog nor send out e-mail. This means it e-mails only once for each user of the computer. W32/Crock-A looks for and shuts down a wide range of security software by finding and killing off processes with various names. W32/Crock-A also creates a file named CROCK.BAT in your startup folder (the file is not hidden). This file is supposed to be a parasitic batch file virus, but does not work correctly.

W32.HLLP.Rosec (Alias: Win32.HLLP.Rosec) Win32 Virus): This is a virus that infects Portable Executable (PE) files. The size of an infected file increases by 16,608 bytes.

W32/Lamud.worm (Win32 Worm): This is a new worm spreading on open network shares. It tries to connect to computers within the local network and copies itself into startup folders. After execution it opens a Explorer window and displays the %Windir% folder. A few seconds later it displays pornographic pictures, which are set as wallpapers on the desktop. It disables access to administrative tools like 'REGEDIT.EXE' and the configuration dialog of the desktop settings.

W32/Lovgate-M (Aliases: I-Worm.LovGate.gen, W95/Lovgate.L@mm, W32/Lovgate.gen@M virus, W32.HLLW.Lovgate.I@mm, PE_LOVGATE.J, W32.HLLW.Lovgate.L@mm, I-Worm.Lovgate.i) (Win32 Worm): W32/Lovgate-M is a minor variant of W32/Lovgate-J.

W32/Magold-D (Alias: I-Worm.Magold.e, W32.HLLW.Magold.E@mm, WORM_AURIC.E, I-Worm.Magold.e) (Win32 Worm): This worm has been reported in the wild. It is a memory resident worm that uses e-mail, IRC channels, network shared drives and P2P network shares to spread. The worm arrives in an e-mail message with subject line and message text of non-Roman characters. If the viral attachment is run, W32/Magold-D displays the message box "DirectX Error! Address:19851022" and copies itself to C:\<Windows>\dreAd.exe, C:\<Windows>\dreAd\Maya Gold.scr, C:\<Windows>\Maya Gold.scr, and C:\<System>\wdread.exe. During the execution of the e-mail routine, the worm sends a notification message to the virus writer containing the IP address, username, computer name and available shares of the infected machine. W32/Magold-D uses the Windows Address Book and HTML files found on the local drive to retrieve e-mail addresses that will be used to send the worm message. All addresses found are stored in the file ravec.txt that will be saved by the worm in the Windows folder. The worm may create a folder dreAd in the Windows folder and attempt to register the folder in the registry as one used as a file repository for a number of P2P clients. W32/Magold-A searches for and terminates processes that belong to several anti-virus products. The worm changes the following registry entries so that the worm file dreAd.exe is run before any file with the extension EXE, PIF, COM, SCR and BAT:

- HKCR\exefile\shell\open\command
- HKCR\comfile\shell\open\command
- HKCR\piffile\shell\open\command
- HKCR\batfile\shell\open\command
- HKCR\scrfile\shell\open\command

W32/Magold-A also creates the registry entry:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\raVe

so that the worm file dreAd.exe is run on Windows startup. The registry entry HKLM\Software\dreAd is used by the worm to store data used internally by the worm. The worm contains several randomly triggered payload routines such as opening the CD-ROM drive tray, changing the Windows color scheme, restricting the movement of the mouse pointer to the lower part of the screen, opening the web page http://www.offspring.com, writing the text "=:-) OFFSPRING is coOL =:-) PUNK'S NOT DEAD =:-)" to the caption area of the topmost window and creating a large number of zero-byte text files on the Desktop.

W32/Magold-D may also send a Hungarian text to be printed on the default printer and may attempt to delete all files with the extension BMP, GIF and JPG from the hard drive. The worm may attempt to copy itself to all local drives, shared network drives and floppy disks (if one is in the floppy disk drive) as Maya Gold.scr and may create the file autorun.inf so that the worm file is run automatically when the drive is opened using Explorer if the autorun feature is enabled. On an infected computer, the two copies of the worm dreAd.exe and wdread.exe run in the background as processes and monitor each other so that if one is terminated, the other restarts it immediately. Furthermore, the registry entries created above are also monitored such that a registry value is immediately restored if it was changed.

W32.Moulo (Alias: W32/Mouseloco.Worm): This is a worm that copies itself to the hard drive and the floppy disk drive. It uses the same icon as Microsoft Word and is written in Microsoft Visual Basic. When W32.Moulo is executed, it copies itself as:

- %Windir%\WinCMI.exe
- A:\IUT-RC-chicas.exe

and adds the value, "WinCMI"="%Windir%\WinCMI.exe." to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

W32/Nofer-A (Aliases: I-Worm.Fearso, Win32/Farex.A, PE_NOFEAR.A, W32/Nofer.A@mm, W95/Fearso.A@mm) (Win32 Worm): This is an Internet worm that will attempt to e-mail itself to addresses found from a variety of sources on the local machine. W32/Nofer-A will also try to infect executable files. W32/Nofer-A will copy itself to svchost.exe and to a randomly named executable file in the Windows folder. It creates a registry entry in:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\

that points to the randomly named executable file to ensure the worm is run at system startup. W32/Nofer-A will also attempt to spread using peer-to-peer networks.

W32/Nofer-B (Win32 Worm): This is an Internet worm that tries to e-mail itself to addresses extracted from a variety of sources on your computer. W32/Nofer-B also infects programs already on your computer. W32/Nofer-B copies itself into your Windows folder, using the filenames svchost.exe (usually 43023 bytes) and kernel.dll (usually 59904 bytes). W32/Nofer-B also copies itself to a randomly-named hidden file (e.g. MWd0veUK.exe) in your Windows folder. The virus then adds a registry entry to:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\

so that this hidden file is launched every time you logon to your computer.

W32/Nofer-C (Aliases: I-Worm.Fearso.c, Win32/Farex.C, PE_NOFEAR.C, W32/Nofer.C@mm, W95/Fearso.C@mm) (Win32 Virus): This is a virus which tries to e-mail itself to addresses extracted from a variety of sources on your computer. W32/Nofer-C also infects programs already on your computer. W32/Nofer-C copies itself into the Windows folder, using the filenames svchost.exe and kernel.dll (usually 66048 bytes). W32/Nofer-C also copies itself to a randomly-named hidden file (e.g. Uhy43cuAqUQ.exe) in your Windows folder. The virus then adds a registry entry to:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\

so that the hidden file is launched every time you logon to your computer.

W32.Randex.C (Aliases: Gesfm, W32/Randex.worm.c) (Win32 Worm): This is a network-aware worm that will copy itself as the following files:

- \Admin$\system32\msmonk32.exe
- \c$\winnt\system32\msmonk32.exe

The worm will receive instructions from an IRC channel on a specific IRC server. One such command will trigger the aforementioned spreading.

W32/Redist-C (Aliases: WORM_GANT.C, W32.RedZed@mm, Win32/OutSid.C, W32.Redzed@mm, I-Worm/Outsider, W32/Outsider.C, W32/Gant.d@MM) (Win32 Worm): This is an Internet worm which spreads by e-mail and over peer-to-peer networks. W32/Redist-C uses Outlook to send itself to entries in your address book. E-mails sent out by the worm have various subject lines, message bodies, and attachments. W32/Redist-C makes itself available over peer-to-peer networks by copying itself to various folders. W32/Redist-C makes two copies of itself to your Windows folder, using the names:

- Mslg32.exe
- Winprg32.pif

The worm copies itself to your System folder, using the name:, “Winlg32.pif .” W32/Redist-C adds this entry to your registry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\SecureLogin

This value is set to launch the file Mslg32.exe every time you log on to your computer. W32/Redist-C also adds the registry entry:

- HKCU\Software\Zed\Outsider\Outsider3 = "W32/Outsider.C by Zed"

W32/Redist-C tries to overwrite files with extensions starting with "MP" and "WM" (these are usually music files). The additional extension ".pif" is added to the filename. Although the filename looks the same as it was, you will launch the virus if you double-click on these files in the future. Note that the original music files are destroyed. You will not easily be able to restore them unless you have a recent backup. W32/Redist-C logs what you type and writes your keystrokes into a file named Mskmap32.txt or Mskmap.txt. The worm then e-mails this file to a Hotmail address. W32/Redist-C looks for and shuts down a wide range of security software by finding and killing off processes with various names.

W32/Sage-A (Alias: BackDoor-ASV) (Win32 Worm): This is a worm that spreads through e-mail attachments. The e-mails have various characteristics. Upon execution, the worm drops a copy of itself as svch0st.exe, and another component as WinSocks.Dll, to the Windows System folder and then removes itself from the current folder. W32/Sage-a sets the following registry entries so that it is run on startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\winsock ="<System>\svch0st.exe"
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\winsock ="<System>\svch0st.exe"

In addition, the worm adds the following entry to win.ini to run itself on startup, “run=<System>\svch0st.exe.” W32/Sage-A worm also modifies the following registry entry so that it is run whenever an executable is run:

- HKCR\exefile\shell\open\command = "<System>\svch0st.exe "%1" %*"

W32/Sage-A opens numerous ports on the local computer and connects to a remote computer. This might provide unauthorized backdoor access from a remote location. W32/Sage-A runs in the background as a process and performs process stealthing, which makes it difficult to terminate the running process.

W32/Sobig-D (Alias: W32/Sobig.dam, W32.Sobig.D@mm, I-Worm.Sobig.gen, W32/Sobig.d@MM, Win32.Sobig.D, WORM_SOBIG.D) (Win32 Worm): This is an Internet worm which spreads by copying itself to the startup folder of network shares and by e-mailing itself to addresses found within locally stored files that have an extension of TXT, EML, HTML, HTM or DBX. The e-mails sent have the various characteristics. W32/Sobig-D spoofs the From: field using e-mail addresses extracted from locally stored files or "admin@support.com.” W32/Sobig-D will not spread if the date is July 2nd 2003 or later. When run, the worm copies itself to the Windows folder as cftrb32.exe and creates the following registry entries so that cftrb32.exe is run automatically each time Windows is started:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SFtrb Service = %WINDOWS%\cftrb32.exe
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\SFtrb Service = %WINDOWS%\cftrb32.exe

The worm enumerates network drives and copies itself to the following startup folders if they are shared with write access:

- Windows\All Users\Start Menu\Programs\Startup
- Documents and Settings\All Users\Start Menu\Programs\Startup

W32/Sobig-D also creates the file rssp32.dat in the Windows folder.

W32/Sobig-E (Aliases: W32/Sobig.e@MM, Sobig.E, Win32.Sobig.E, W32.Sobig.e@mm, WORM_SOBIG.E) (Win32 Worm): This worm has been reported in the wild. It arrives via e-mail and attempts to travel via network shares. The worm sends itself as an attachment to e-mail addresses collected from infected computers. W32/Sobig-E may spoof the From field of the sent e-mails using the e-mail address support@yahoo.com or addresses collected from the user's computer. When run W32/Sobig-E copies itself into the Windows folder as winssk32.exe and sets the following registry entries:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SSK Service = <Windows folder>\winssk32.exe
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SSK Service = <Windows folder>\winssk32.exe

W32/Sobig-E will not spread if the date is 14th July or later.

W32/Specx.worm (Win32 Worm): This is an Internet worm that propagates via KaZaA and iMesh peer-to-peer network. When run, the worm displays a fake error message. The worm copies itself into %WinDir%/system32 directory as “iexplore32.exe” and creates the following registry key in order to load itself as Windows startup:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "IELoader32" = "iexplore32.exe"

The worm adds/modifies the following registry keys to enable P2P file sharing:

- HKEY_CURRENT_USER\Software\iMesh\Client\LocalContent "Dir0" = 012345:C:\WINNT\System32\drivers32\
- HKEY_CURRENT_USER\Software\KAZAA\LocalContent "Dir0" = 012345:C:\WINNT\System32\drivers32\

It creates the following directory, “%Windir%\system32\drivers32,” and copies itself into the directory as various files.

W32/Yaha-T (Aliases: WORM_YAHA.N, W32/Yaha.t@MM, I-Worm.Lentis.gen,) (Win32 Worm): This is a worm which spreads by e-mailing itself via SMTP to addresses extracted from various sources on the victim's computer, by copying itself to network shares and by copying itself to other fixed drives connected to the computer. The worm copies itself to the Windows system folder as WINTSK32.EXE and EXELDR32.EXE and adds the following registry entries to run itself on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\MicrosoftServiceManager = <Windows system>\WINTSK32.EXE
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\MicrosoftServiceManager = <Windows system>\WINTSK32.EXE

W32/Yaha-T also changes the entry in the registry at HKCR\exefile\shell\open\command so that the worm is run before all EXE files. W32/Yaha-T attempts to exploit the IFRAME vulnerability in certain versions of Microsoft Internet Explorer and Outlook Express that allows automatic execution of files attached to e-mails when the e-mail is viewed. The From field of the e-mails is randomly constructed from a list of names and e-mail addresses. W32/Yaha-T copies itself to fixed drives connected to the computer and to remote network shares as <Windows>\REG32.EXE and <Documents and Settings\All Users\Start Menu\Programs\Startup>\MSREGSCANNER.EXE and changes the WIN.INI so that REG32.EXE is run when the system is restarted. The worm shuts down windows with the names "Process Viewer,” "Registry Editor,” "System Configuration Utility" and "Windows Task Manager.” W32/Yaha-T also deletes files and registry entries related to certain types of software. W32/Yaha-T may also drop a DLL plugin that allows it to record keystrokes that may subsequently be e-mailed to an external address. The worm may also attempt a denial-of-service attack on the following URLs:

- finance.gov.pk
- forisb.org
- jamatdawa.org
- interior.gov.pk
- infopak.gov.pk

WM97/Relax-C (Word 97 Macro Virus): On the 10th, 20th, and 30th of April, August, and December, WM97/Relax-C attempts to append code to C:\autoexec.bat. It uses the file C:\temp.tmp to replicate.

WM97/Simuleek-B (Aliases: Macro.Word97.Omni, W97M.Radnet.B, W97M_BUHAY.A, W97M/Simuleek.B) (Word 97 Macro Virus): This virus creates a VBScript file called WordSeek.vbs in the Windows folder which it uses to infect Word files. The virus adds a line to win.ini to run this VBScript, which is detected as VBS/Simuleek-B.

Worm/Evan (Internet Worm): This is an Internet worm that spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book. If executed, the worm copies itself in the \windows\ directory under the filename "eva.exe." Additionally, the file "vbs.eva.vbs (2.335 bytes)" gets added in the \windows\ directory. So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "Eva"="C:\\WINDOWS\\Eva.exe"

WORM_GANT.B (Aliases: Win32/HLLW.Redist.A, Win32.Thaprog.B) (Internet Worm): This mass-mailer is a variant of WORM_GANT.A. It similarly spreads via e-mail using Microsoft Outlook and through popular peer-to-peer file-sharing networks such as KaZaA. It also terminates certain antivirus programs and is capable of stealing passwords from infected users then sends it to the malware author.

Worm/Merkur.D (Alias: I-Worm.Merkur.d) (Internet Worm): This is an Internet worm that spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book, as well as, through various file-sharing programs including KaZaA and eDonkey2000. The worm arrives through e-mail in the following format:

- Subject: E-mail Virus Remover
- Attachment: TASKMAN.EXE

If executed, the worm copies itself in the various locations. So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run] "Swf32"="C:\\Windows\\AVupdate.exe"

WORM_MUMU.A (Aliases: W32.Mumu.B.Worm, W32/Mumu.b.worm) (Internet Worm): This worm attempts to spread by locating SMB shares. It penetrates these shares using a list of weak administrator passwords. To carry out its malicious routines, this worm drops several files upon execution, including two malware components detected as BAT_SPYBOT.A and TROJ_HACLINE.A. The worm uses two ways to infiltrate host systems: via remote connection and local shared connection. Remote connection is done through IP scanning, while local shared connection is done by finding established connections to copy and execute its malicious program. It runs under Windows 95, 98, ME, 2000, XP and NT, but successfully replicates only in Windows NT, 2000 and XP due to its target shared folder which is only available under the said platforms.

Worm.Win32.Sluter (Win32 Worm): Sluter is a worm virus that spreads over Win32 networks through shared resources. The worm is a Windows PE EXE file about 18KB in length (when compressed by UPX, the decompressed size is about 45KB). It is written in Microsoft Visual C++. When the infected file is run the worm registers itself in the system registry auto-run key:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run superslut = { worm file name }

Next, Sluter runs its spreading routines. The spreading routine runs up to 60 "threads" which scan port 445 at random IP addresses. When successfully connecting to a victim machine it tries to locate open resources on the remote computer and connects to them using several passwords such as: "","admin," "root," "123," etc.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Note: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #

Trojan	Version	CyberNotes Issue #
AdwareDropper-A	A	CyberNotes-2003-04
AIM-Canbot	N/A	CyberNotes-2003-07
AprilNice	N/A	CyberNotes-2003-08
Backdoor.Acidoor	N/A	CyberNotes-2003-05
Backdoor.Amitis	N/A	CyberNotes-2003-01
Backdoor.Amitis.B	B	CyberNotes-2003-11
Backdoor.AntiLam.20.K	K	CyberNotes-2003-10
Backdoor.Apdoor	N/A	CyberNotes-2003-12
Backdoor.Assasin.D	D	CyberNotes-2003-01
Backdoor.Assasin.E	E	CyberNotes-2003-04
Backdoor.Assasin.F	F	CyberNotes-2003-09
Backdoor.Badcodor	N/A	CyberNotes-2003-12
Backdoor.Beasty	N/A	CyberNotes-2003-02
Backdoor.Beasty.B	B	CyberNotes-2003-03
Backdoor.Beasty.C	C	CyberNotes-2003-05
Backdoor.Beasty.Cli	Cli	CyberNotes-2003-10
Backdoor.Beasty.D	D	CyberNotes-2003-06
Backdoor.Beasty.E	E	CyberNotes-2003-06
Backdoor.Bigfoot	N/A	CyberNotes-2003-09
Backdoor.Bmbot	N/A	CyberNotes-2003-04
Backdoor.Bridco	N/A	CyberNotes-2003-06
Backdoor.CamKing	N/A	CyberNotes-2003-10
Backdoor.CHCP	N/A	CyberNotes-2003-03
Backdoor.Cmjspy	N/A	CyberNotes-2003-10
Backdoor.CNK.A	A	CyberNotes-2003-10
Backdoor.CNK.A.Cli	Cli	CyberNotes-2003-10
Backdoor.Colfuser	N/A	CyberNotes-2003-01
Backdoor.Cow	N/A	CyberNotes-2003-01
Backdoor.Cybspy	N/A	CyberNotes-2003-01
Backdoor.Dani	N/A	CyberNotes-2003-04
Backdoor.Darmenu	N/A	CyberNotes-2003-05
Backdoor.Death.Cli	Cli	CyberNotes-2003-10
Backdoor.Deftcode	N/A	CyberNotes-2003-01
Backdoor.Delf.Cli	Cli	CyberNotes-2003-10
Backdoor.Delf.F	F	CyberNotes-2003-07
Backdoor.Drator	N/A	CyberNotes-2003-01
Backdoor.Dvldr	N/A	CyberNotes-2003-06
Backdoor.EggDrop	N/A	CyberNotes-2003-08
Backdoor.Fatroj	N/A	CyberNotes-2003-10
Backdoor.Fatroj.Cli	Cli	CyberNotes-2003-10
Backdoor.Fluxay	N/A	CyberNotes-2003-07
Backdoor.FTP.Casus	N/A	CyberNotes-2003-02
Backdoor.FTP_Ana.C	C	CyberNotes-2003-07
Backdoor.FTP_Ana.D	D	CyberNotes-2003-08
Backdoor.Fxdoor	N/A	CyberNotes-2003-10
Backdoor.Fxdoor.Cli	Cli	CyberNotes-2003-10
Backdoor.Graybird	N/A	CyberNotes-2003-07
Backdoor.Graybird.B	B	CyberNotes-2003-08
Backdoor.Graybird.C	C	CyberNotes-2003-08

Trojan	Version	CyberNotes Issue #
Backdoor.Grobodor	N/A	CyberNotes-2003-12
Backdoor.HackDefender	N/A	CyberNotes-2003-06
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hipo	N/A	CyberNotes-2003-04
Backdoor.Hitcap	N/A	CyberNotes-2003-04
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	CyberNotes-2003-02
Backdoor.IRC.Cloner	N/A	CyberNotes-2003-04
Backdoor.IRC.Comiz	N/A	CyberNotes-2003-11
Backdoor.IRC.Lampsy	N/A	CyberNotes-2003-10
Backdoor.IRC.Ratsou	N/A	CyberNotes-2003-10
Backdoor.IRC.Ratsou.B	B	CyberNotes-2003-11
Backdoor.IRC.Ratsou.C	C	CyberNotes-2003-11
Backdoor.IRC.Yoink	N/A	CyberNotes-2003-05
Backdoor.IRC.Zcrew	N/A	CyberNotes-2003-04
Backdoor.Kaitex.D	D	CyberNotes-2003-09
Backdoor.Kalasbot	N/A	CyberNotes-2003-09
Backdoor.Khaos	N/A	CyberNotes-2003-04
Backdoor.Kilo	N/A	CyberNotes-2003-04
Backdoor.Kol	N/A	CyberNotes-2003-06
Backdoor.Krei	N/A	CyberNotes-2003-03
Backdoor.Lala	N/A	CyberNotes-2003-01
Backdoor.LeGuardien.B	B	CyberNotes-2003-10
Backdoor.Litmus.203.c	c	CyberNotes-2003-09
Backdoor.LittleWitch.C	C	CyberNotes-2003-06
Backdoor.Longnu	N/A	CyberNotes-2003-06
Backdoor.Marotob	N/A	CyberNotes-2003-06
Backdoor.Massaker	N/A	CyberNotes-2003-02
Backdoor.Monator	N/A	CyberNotes-2003-08
Backdoor.Mots	N/A	CyberNotes-2003-11
Backdoor.MSNCorrupt	N/A	CyberNotes-2003-06
Backdoor.NetDevil.B	B	CyberNotes-2003-01
Backdoor.NetTrojan	N/A	CyberNotes-2003-01
Backdoor.Ohpass	N/A	CyberNotes-2003-01
Backdoor.OICQSer.165	N/A	CyberNotes-2003-01
Backdoor.OICQSer.17	17	CyberNotes-2003-01
Backdoor.Optix.04.d	04.d	CyberNotes-2003-04
Backdoor.OptixDDoS	N/A	CyberNotes-2003-07
Backdoor.OptixPro.10.c	10.c	CyberNotes-2003-01
Backdoor.OptixPro.12.b	12.b	CyberNotes-2003-07
Backdoor.OptixPro.13	13	CyberNotes-2003-09
Backdoor.Peers	N/A	CyberNotes-2003-10
Backdoor.Plux	N/A	CyberNotes-2003-05
Backdoor.Pointex	N/A	CyberNotes-2003-09
Backdoor.Pointex.B	B	CyberNotes-2003-09
Backdoor.Private	N/A	CyberNotes-2003-11
Backdoor.Prorat	**N/A**	**Current Issue**
Backdoor.PSpider.310	310	CyberNotes-2003-05

Trojan	Version	CyberNotes Issue #
Backdoor.Queen	N/A	CyberNotes-2003-06
Backdoor.Ratega	N/A	CyberNotes-2003-09
Backdoor.Recerv	N/A	CyberNotes-2003-09
Backdoor.Redkod	N/A	CyberNotes-2003-05
Backdoor.Remohak.16	16	CyberNotes-2003-01
Backdoor.RemoteSOB	N/A	CyberNotes-2003-01
Backdoor.Rephlex	N/A	CyberNotes-2003-01
Backdoor.Rsbot	N/A	CyberNotes-2003-07
Backdoor.SchoolBus.B	B	CyberNotes-2003-04
Backdoor.Sdbot.C	C	CyberNotes-2003-02
Backdoor.Sdbot.D	D	CyberNotes-2003-03
Backdoor.Sdbot.E	E	CyberNotes-2003-06
Backdoor.Sdbot.F	F	CyberNotes-2003-07
Backdoor.Sdbot.G	G	CyberNotes-2003-08
Backdoor.Sdbot.H	H	CyberNotes-2003-09
Backdoor.Sdbot.L	L	CyberNotes-2003-11
Backdoor.Sdbot.M	**M**	**Current Issue**
Backdoor.Serpa	N/A	CyberNotes-2003-03
Backdoor.Servsax	N/A	CyberNotes-2003-01
Backdoor.SilverFTP	N/A	CyberNotes-2003-04
Backdoor.Simali	N/A	CyberNotes-2003-09
Backdoor.Sixca	N/A	CyberNotes-2003-01
Backdoor.Slao	N/A	CyberNotes-2003-11
Backdoor.Snami	N/A	CyberNotes-2003-10
Backdoor.Snowdoor	N/A	CyberNotes-2003-04
Backdoor.Socksbot	N/A	CyberNotes-2003-06
Backdoor.Softshell	N/A	CyberNotes-2003-10
Backdoor.SubSari.15	15	CyberNotes-2003-05
Backdoor.SubSeven.2.15	2.15	CyberNotes-2003-05
Backdoor.Syskbot	N/A	CyberNotes-2003-08
Backdoor.SysXXX	N/A	CyberNotes-2003-06
Backdoor.Talex	N/A	CyberNotes-2003-02
Backdoor.Tankedoor	N/A	CyberNotes-2003-07
Backdoor.Trynoma	N/A	CyberNotes-2003-08
Backdoor.Turkojan	N/A	CyberNotes-2003-07
Backdoor.Udps.10	1	CyberNotes-2003-03
Backdoor.UKS	N/A	CyberNotes-2003-11
Backdoor.Unifida	N/A	CyberNotes-2003-05
Backdoor.Upfudoor	N/A	CyberNotes-2003-01
Backdoor.VagrNocker	N/A	CyberNotes-2003-01
Backdoor.Vmz	N/A	CyberNotes-2003-01
Backdoor.Winet	N/A	CyberNotes-2003-11
Backdoor.Xenozbot	N/A	CyberNotes-2003-01
Backdoor.Xeory	N/A	CyberNotes-2003-03
Backdoor.XTS	N/A	CyberNotes-2003-08
Backdoor.Zdemon	N/A	CyberNotes-2003-02
Backdoor.Zdemon.126	126	CyberNotes-2003-10
Backdoor.Zdown	N/A	CyberNotes-2003-05
Backdoor.Zix	N/A	CyberNotes-2003-02

Trojan	Version	CyberNotes Issue #
Backdoor.Zombam	N/A	CyberNotes-2003-08
Backdoor.Zvrop	N/A	CyberNotes-2003-03
Backdoor-AFC	N/A	CyberNotes-2003-05
Backdoor-AOK	N/A	CyberNotes-2003-01
BackDoor-AQL	N/A	CyberNotes-2003-05
BackDoor-AQT	N/A	CyberNotes-2003-05
BackDoor-ARR	ARR	CyberNotes-2003-06
Backdoor-ARU	ARU	CyberNotes-2003-06
BackDoor-ARX	ARX	CyberNotes-2003-06
BackDoor-ARY	ARY	CyberNotes-2003-06
BackDoor-ASD	ASD	CyberNotes-2003-07
BackDoor-ASL	ASL	CyberNotes-2003-07
BackDoor-ASW	ASW	CyberNotes-2003-08
BackDoor-ATG	ATG	CyberNotes-2003-09
BackDoor-AUP	N/A	CyberNotes-2003-11
BackDoor-AVF	AVF	CyberNotes-2003-12
BackDoor-AVH	AVH	CyberNotes-2003-12
BackDoor-AVO	AVO	CyberNotes-2003-12
BDS/AntiPC	N/A	CyberNotes-2003-02
BDS/Backstab	N/A	CyberNotes-2003-02
BDS/CheckESP	N/A	CyberNotes-2003-12
BDS/Ciadoor.10	10	CyberNotes-2003-07
BDS/Evilbot.A	A	CyberNotes-2003-09
BDS/Evolut	N/A	CyberNotes-2003-03
BDS/PowerSpider.A	A	CyberNotes-2003-11
Daysun	N/A	CyberNotes-2003-06
DDoS-Stinkbot	N/A	CyberNotes-2003-08
DoS-iFrameNet	N/A	CyberNotes-2003-04
Download.Trojan.B	**B**	**Current Issue**
Downloader.BO.B	B	CyberNotes-2003-10
Downloader.BO.B.dr	B.dr	CyberNotes-2003-10
Downloader-BN.b	**BN.b**	**Current Issue**
Downloader-BO.dr.b	N/A	CyberNotes-2003-02
Downloader-BS	N/A	CyberNotes-2003-02
Downloader-BW	N/A	CyberNotes-2003-05
Downloader-BW.b	BW.b	CyberNotes-2003-06
Downloader-BW.c	BW.c	CyberNotes-2003-07
ELF_TYPOT.A	**A**	**Current Issue**
ELF_TYPOT.B	**B**	**Current Issue**
Exploit-IISInjector	N/A	CyberNotes-2003-03
Gpix	N/A	CyberNotes-2003-08
Hacktool.PWS.QQPass	N/A	CyberNotes-2003-06
ICQPager-J	N/A	CyberNotes-2003-05
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	CyberNotes-2003-02
IRC/Backdoor.g	g	CyberNotes-2003-03
IRC/Flood.ap	N/A	CyberNotes-2003-05
IRC/Flood.bi	N/A	CyberNotes-2003-03

Trojan	Version	CyberNotes Issue #
IRC/Flood.br	br	CyberNotes-2003-06
IRC/Flood.bu	bu	CyberNotes-2003-08
IRC/Flood.cd	cd	CyberNotes-2003-11
IRC/Flood.cm	**cm**	**Current Issue**
IRC-Emoz	N/A	CyberNotes-2003-03
IRC-OhShootBot	N/A	CyberNotes-2003-01
IRC-Vup	N/A	CyberNotes-2003-09
JS.Fortnight.B	B	CyberNotes-2003-06
JS.Seeker.J	J	CyberNotes-2003-01
JS/Fortnight.c@M	c	CyberNotes-2003-11
JS/Seeker-C	C	CyberNotes-2003-04
JS/StartPage.dr	dr	CyberNotes-2003-11
JS_WEBLOG.A	A	CyberNotes-2003-05
KeyLog-Kerlib	N/A	CyberNotes-2003-05
Keylog-Kjie	N/A	CyberNotes-2003-12
Keylog-Perfect.dr	dr	CyberNotes-2003-09
Keylog-Razytimer	N/A	CyberNotes-2003-03
KeyLog-TweakPan	N/A	CyberNotes-2003-02
Keylog-Yeehah	N/A	CyberNotes-2003-12
Linux/Exploit-SendMail	N/A	CyberNotes-2003-05
MultiDropper-FD	N/A	CyberNotes-2003-01
Pac	N/A	CyberNotes-2003-04
ProcKill-AE	N/A	CyberNotes-2003-05
ProcKill-AF	N/A	CyberNotes-2003-05
ProcKill-AH	AH	CyberNotes-2003-08
ProcKill-AJ	**AJ**	**Current Issue**
ProcKill-Z	N/A	CyberNotes-2003-03
Proxy-Guzu	N/A	CyberNotes-2003-08
PWS-Aileen	N/A	CyberNotes-2003-04
PWSteal.ABCHlp	N/A	CyberNotes-2003-12
PWSteal.AlLight	N/A	CyberNotes-2003-01
PWSteal.Hukle	N/A	CyberNotes-2003-08
PWSteal.Kipper	N/A	CyberNotes-2003-10
PWSteal.Lemir.105	105	CyberNotes-2003-10
PWSteal.Rimd	N/A	CyberNotes-2003-01
PWSteal.Rimd.B	B	CyberNotes-2003-10
PWSteal.Senhas	N/A	CyberNotes-2003-03
PWSteal.Snatch	N/A	CyberNotes-2003-10
PWSteal.Sysrater	N/A	CyberNotes-2003-12
PWS-Tenbot	N/A	CyberNotes-2003-01
PWS-Truebf	**N/A**	**Current Issue**
PWS-Watsn	N/A	CyberNotes-2003-10
PWS-WMPatch	N/A	CyberNotes-2003-07
PWS-Yipper	N/A	CyberNotes-2003-10
QDel359	359	CyberNotes-2003-01
QDel373	373	CyberNotes-2003-06
Qdel374	374	CyberNotes-2003-06
Qdel375	375	CyberNotes-2003-06
Qdel376	376	CyberNotes-2003-07

Trojan	Version	CyberNotes Issue #
QDel378	378	CyberNotes-2003-08
QDel379	369	CyberNotes-2003-09
QDel390	**390**	**Current Issue**
QDel391	**391**	**Current Issue**
QDel392	**392**	**Current Issue**
QDial6	6	CyberNotes-2003-11
Renamer.c	N/A	CyberNotes-2003-03
Reom.Trojan	N/A	CyberNotes-2003-08
StartPage-G	G	CyberNotes-2003-06
Startpage-N	**N**	**Current Issue**
Stoplete	N/A	CyberNotes-2003-06
Swizzor	N/A	CyberNotes-2003-07
Tellafriend.Trojan	N/A	CyberNotes-2003-04
Tr/Decept.21	21	CyberNotes-2003-07
Tr/DelWinbootdir	N/A	CyberNotes-2003-07
TR/Fake.YaHoMe.1	N/A	CyberNotes-2003-02
Tr/SpBit.A	A	CyberNotes-2003-04
Tr/VB.t	T	CyberNotes-2003-11
TR/WinMx	N/A	CyberNotes-2003-02
Troj/Dloader-BO	BO	CyberNotes-2003-02
Troj/Hacline-B	**B**	**Current Issue**
Troj/IRCBot-C	C	CyberNotes-2003-11
Troj/Manifest-A	N/A	CyberNotes-2003-03
Troj/Mystri-A	**A**	**Current Issue**
Troj/PcGhost-A	**A**	**Current Issue**
Troj/Peido-B	B	CyberNotes-2003-10
Troj/Qzap-248	N/A	CyberNotes-2003-01
Troj/SadHound-A	N/A	CyberNotes-2003-03
Troj/Slacker-A	A	CyberNotes-2003-05
Troj/Slanret-A	N/A	CyberNotes-2003-03
Troj/TKBot-A	A	CyberNotes-2003-04
TROJ_JBELLZ.A	A	CyberNotes-2003-02
TROJ_KILLBOOT.B	B	CyberNotes-2003-01
TROJ_RACKUM.A	A	CyberNotes-2003-05
Trojan.AprilFool	N/A	CyberNotes-2003-08
Trojan.Barjac	N/A	CyberNotes-2003-05
Trojan.Dasmin	N/A	CyberNotes-2003-01
Trojan.Dasmin.B	B	CyberNotes-2003-03
Trojan.Downloader.Aphe	N/A	CyberNotes-2003-06
Trojan.Downloader.Inor	N/A	CyberNotes-2003-02
Trojan.Grepage	N/A	CyberNotes-2003-05
Trojan.Guapeton	N/A	CyberNotes-2003-08
Trojan.Idly	N/A	CyberNotes-2003-04
Trojan.Ivanet	N/A	CyberNotes-2003-02
Trojan.Kaht	N/A	CyberNotes-2003-10
Trojan.KKiller	N/A	CyberNotes-2003-01
Trojan.Lear	N/A	CyberNotes-2003-10
Trojan.Mumuboy	**N/A**	**Current Issue**

Trojan	Version	CyberNotes Issue #
Trojan.Myet	N/A	CyberNotes-2003-12
Trojan.Poldo.B	B	CyberNotes-2003-02
Trojan.Poot	N/A	CyberNotes-2003-05
Trojan.PopSpy	N/A	CyberNotes-2003-11
Trojan.ProteBoy	N/A	CyberNotes-2003-04
Trojan.PSW.Gip	N/A	CyberNotes-2003-06
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	CyberNotes-2003-02
Trojan.Qforager	N/A	CyberNotes-2003-02
Trojan.Qforager.Dr	N/A	CyberNotes-2003-02
Trojan.Qwe	N/A	CyberNotes-2003-02
Trojan.Sidea	N/A	CyberNotes-2003-12
Trojan.Snag	N/A	CyberNotes-2003-02
Trojan.Unblockee	N/A	CyberNotes-2003-01
Uploader-D	D	CyberNotes-2003-06
Uploader-D.b	D.b	CyberNotes-2003-07
VBS.ExitWin	N/A	CyberNotes-2003-12
VBS.Kasnar	N/A	CyberNotes-2003-06
VBS.Moon.B	B	CyberNotes-2003-02
VBS.StartPage	N/A	CyberNotes-2003-02
VBS.Trojan.Lovcx	N/A	CyberNotes-2003-05
VBS.Zizarn	N/A	CyberNotes-2003-09
VBS/Fourcourse	N/A	CyberNotes-2003-06
W32.Adclicker.C.Trojan	C	CyberNotes-2003-09
W32.Benpao.Trojan	N/A	CyberNotes-2003-04
W32.CVIH.Trojan	N/A	CyberNotes-2003-06
W32.Noops.Trojan	N/A	CyberNotes-2003-09
W32.Socay.Worm	N/A	CyberNotes-2003-02
W32.Systentry.Trojan	N/A	CyberNotes-2003-03
W32.Xilon.Trojan	N/A	CyberNotes-2003-01
W32.Yinker.Trojan	N/A	CyberNotes-2003-04
W32/Igloo-15	N/A	CyberNotes-2003-04
Xin	N/A	CyberNotes-2003-03

Backdoor.Prorat (Alias: Backdoor.Prorat.10b3): This is a Backdoor Trojan Horse that gives its creator full control over your computer. It opens port 58343 by default. It is written in the Delphi programming language and is packed with UPX. When Backdoor.Prorat is executed, it copies itself as the following files in the %System% folder:

- Main.exe
- Loader.exe
- Msmsg.exe

and adds the value, "MSNMESENGER"="%System%\Main.exe," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

The Trojan sends the version number of the Trojan and the IP address and port number of the target computer to a specific ICQ user through the ICQ Web pager.

Backdoor.Sdbot.M: This is a Backdoor Trojan Horse that is a variant of Backdoor.Sdbot. It allows the Trojan's creator to use Internet Relay Chat (IRC) to gain access to an infected computer. The original filename may be svsghost.exe. Backdoor.Sdbot.M is UPX-packed. This variant is downloaded by Download.Trojan.B. When Backdoor.Sdbot.M runs, it copies itself to %System%\wsock32p.exe and adds the value, “WSock32 Protocol"="%system%\wsock32p.exe.” to the registry keys:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

The Trojan uses its own IRC client to connect to a specified IRC channel and waits for the commands.

Download.Trojan.B: This is a Trojan Horse that downloads and executes Backdoor.Sdbot.M. The original filename may be update0932.exe. It is written in the Borland Delphi language and is UPX-packed. When Download.Trojan.B runs, it copies itself to %Windir%\regsvs32.exe and adds the value, "Regsvs Services"="%windir%\regsvs32.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

The Trojan then downloads a file detected as Backdoor.Sdbot.M and executes it.

Downloader-BN.b (Alias: TrojanDownloader:Win32/Zasil): This Trojan pretends to be the latest patch from Microsoft and is believed to have been SPAMmed to many users. The URL inside the message is not an official Microsoft site and if visited, the Downloader-BN.b Trojan (named UPDATE0932.EXE) is downloaded. The Trojan copies itself as 'REGSVS32.EXE' in to the %Windir% folder. Many instances of Internet Explorer downloading this file are displayed which results to bringing the machine to a halt. 'UPDATE0932.EXE' is a downloader that retrieves a text file, rq.txt from a remote server. The text file contains a path to another remote file (Note: this path may be modified by the malicious user at anytime). This remote file is downloaded and executed. Since the contents of RQ.TXT may vary, the exact file downloaded is unpredictable. The downloader Trojan hooks system startup by adding one of the following registry keys:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "Regsvs Services"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run "0"

Setting them to point to the installed downloader, “%WinDir%\REGSVS32.EXE.”

ELF_TYPOT.A (Aliases: Stumbler, 55808, Trojan.Linux.Typot): This Linux Trojan is a network sniffer that sends TCP SYN packets with a window size of 55808 to randomly picked destination IP addresses and ports. It spoofs its source IP address and port, making it difficult to trace. This Trojan sniffs the network in promiscuous mode for TCP packets with a window size of 55808. It saves the packets into a file and then sends the file to a specific IP address and port.

ELF_TYPOT.B (Aliases: Stumbler, 55808, Trojan.Linux.Typot): This Linux Trojan is a variant of ELF_TYPOT.A. Its features and functionality are very similar to the A variant except that it contains debug information. This Linux Trojan is a network sniffer that sends TCP SYN packets with a window size of 55808 to randomly picked destination IP addresses and ports. It spoofs its source IP address and port, making it difficult to trace. This Trojan sniffs the network in promiscuous mode for TCP packets with a window size of 55808. It saves the packets into a file and then sends the file to a specific IP address and port.

IRC/Flood.cm (Alias: IRC/Flood.cm.dr): The malware package is delivered to the victim machine via a self-extracting archive dropper (detected as IRC/Flood.cm.dr by the specified DATs). The filename and size of this dropper may change, but one variant received by AVERT had the following characteristics:

- RMTCFG-1.EXE (3,565,056 bytes) - WinZip SFX

ProcKill-AJ: This Trojan exists as a simple batch file. It attempts to terminate anti-virus software, and delete various virus definition files.

PWS-Truebf: The Trojan attempts to gather Login details and Computer name and is sent to the author.

QDel390 (Alias: Trojan.Win32.KillWin.n): When the QDel390 Trojan is run, it tries to modify/delete the files:

- C:\windows\win.ini
- C:\windows\win.vbs
- C:\windows\system.ini
- C :\windows\system32\cmd.exe
- C:\windows\system32\taskmgr.exe

As well as modifying the keyboard/mouse drivers making the system practically unusable.

QDel391 (Alias: Trojan.Win32.VB.ai): When run, no GUI message boxes appear, it runs silently. It may drop the file intrenet.exe in the windows\%system folder and create a registry entry under:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\ "Internet"

It may also change the Internet Explorer startup page, the exact address is omitted on purpose here.

QDel392 (Aliases: Trojan.Win32.VB.aj, Trojan.Xplorer): When run, it may drop itself as explorer.exe in the current directory, initially as a zero bytes file but with increasing filesize due to logging. During testing, this file became over 2 Mb in size. It drops itself as winlogger.exe (24,576 bytes) in the %windows\%system directory and creates a registry key to called:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\

Startpage-N: On executing the Trojan, the following files will be copied:

- windows directory\msinfer.exe
- windows SYSTEM directory\intenats.exe
- windows SYSTEM directory\sysfile.exe
- windows SYSTEM directory\widows.exe

The following registry keys will also be modified:

- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows "load" [windows SYSTEM directory]\widows.exe
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "intenats" [windows SYSTEM directory]\intenats.exe
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "sysfile" [windows SYSTEM directory]\sysfile.exe
- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main "Start Page" http://www.qq3344.com/

The Trojan will also modify win.ini to execute the Trojan on startup:

- run = windows directory\msinfer.exe.

Troj/Hacline-B: This Trojan can be used by intruders to gain unauthorized access to a remote computer. The Trojan attempts to connect to remote computers using a set of passwords listed in a file called IPCPASS.TXT.

Troj/Mystri-A (Alias: TROJ_SYSTRIM.A, Sniff-Systrim, Trojan.Spy.Systrim, Trojan.Systrim): Troj/Mystri-A listens on port 6000 and logs all traffic to the file c:\logfile.txt. At regular intervals the Trojan sends the collected data to a specific e-mail address. In order to be run automatically when Windows starts up the Trojan copies itself to the file systrimit.exe in the Windows system folder and creates the following registry entry to point to this file:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\systrimit

Troj/PcGhost-A: Troj/PcGhost-A is a configurable password stealing Trojan which logs keystrokes and steals confidential information, sending them to a pre-configured e-mail address.

Trojan.Mumuboy (Alias: PWS-SinCom): This is a Trojan Horse that steals information from an infected computer and e-mails this information to the person who created the Trojan. This Trojan is carried by W32.Mumu.B.Worm. When Trojan.Mumuboy is executed, it creates the semaphore object, "qjaashyuhv1.0," to allow only one instance of the Trojan to execute in memory. If the infected computer is running Windows 95/98/ME, the Trojan registers itself as a service process. It copies itself as %Windir%\bboy.exe and inserts the file, %System%\bboy.dll. The Trojan steals information from an infected computer and e-mails it to the person who created the Trojan. Next it starts an infinite loop to set the value to, “Kernel"="%Windir%\bboy.exe,” in the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

It attempts to terminate the following processes: pfw.exe, Iparmor.exe, Eghost.exe, PasswordGuard.exe, DFVSNET.EXE, Kvfw.exe, and kvapfw.exe